F-Response Universal Manual

8.7.1.27

Provides a complete breakdown of leveraging F-Response Universal to perform expert remote e-discovery, computer forensics, and incident response.

Contents

Terminology

The term “Server” refers to both the physical and virtual versions of the F-Response Universal Server software product. The F-Response Universal terms “Examiner”, “Subject” and “Target” are used throughout this manual. The definitions for Examiner, Subject and Target used in this manual are as follows:

Examiner

F-Response Universal Examiner refers to the applications used to connect to the F-Response Universal Appliance and attach remote devices and shares.

Subject

F-Response Universal Subject refers to the applications used to present remote devices, drives, memory and shares to Examiners as defined above.

Target

F-Response Universal Targets refer to individual devices, shares, and data sources presented by Subjects to Examiners as defined above.

Supported Platforms

The F-Response Universal Subject executables are designed to provide all or a subset of the available target types on the following operating systems:

Microsoft Windows (XP, 2003, Vista, 2008, 7, 2008r2, 2012, 8, 2012r2, 10, 11, 2016. 2019, 2022) both 32 and 64-bit

Linux (Most modern distributions, using glibc 2.3.5 or better)

*Apple OSX (10.3+ for command line) **Note: SIP must be disabled for OSX 10.13+, Apple M1 chip is not supported.**

The F-Response Universal Examiner tools can be installed and run on:

Microsoft Windows (10, 11, 2012, 2016, 2019, 2022)

Debian and RPM x86_64 packages (Tested on Centos 6/7, Debian 8, Ubuntu Desktop 14/16, and SIFT3).

The F-Response Universal Server can be run on:

Windows (10, 11, 2012, 2016, 2019, 2022)

Redhat/Centos Linux 7/8/9 64-bit only

Overview

F-Response Universal is a server-based product provided by F-Response which leverages our patented drive technology to provide access to remote systems virtually anywhere in your network. F-Response Universal provides near instant access to Windows, Linux, and Apple OSX devices virtually regardless of the location provided they have network access.

F-Response Universal Server

Hardware Requirements

The largest overall indicator of performance is the CPU cores (virtual or physical) dedicated to the server. More cores translate to more active data connections through the server. A good rule of thumb is two active connections per core.

Recommended hardware configuration:

- 4-8 Cores
- 4-8 Gigabytes of RAM
- 20 Gigabytes of Drive Storage
- 1+ Gigabit Ethernet ports

F-Response Universal License Validation

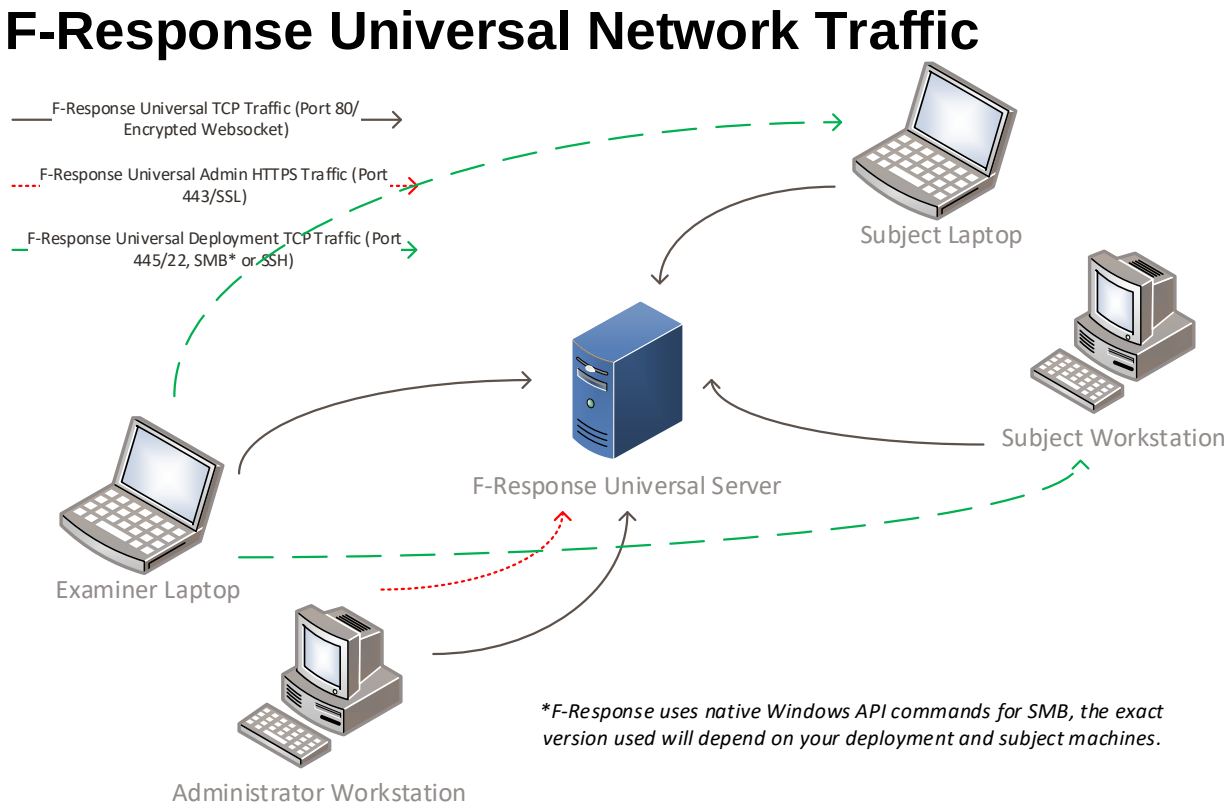
The F-Response Universal Server license is tied to the hardware of the server it is installed on and requires the IP and MAC address(es) are static/reserved for the machine. The F-Response Universal server must be able to contact license.f-response.com on TCP port 443 in order to maintain license validity. You may configure the proxy settings if your organization requires use of a proxy to connect to internet-based servers.

Network Ports and Traffic

F-Response Universal communication occurs over TCP Port 80 by default, is AES-256bit encrypted, and is routed through the Universal Server.

Deployment communication (pushing F-Response subject software to remote machines) occurs directly between the examiner and subject computer over Port 445 for Windows subject computers and Port 22 for Non-Windows computers.

Administration of the Universal server is done using the F-Response Configuration Tool over Port 443 (SSL).



Getting started with the F-Response Universal server

Installation Prep and Licensing

The F-Response Universal Server license is tied to the networking hardware of the server it is installed on. It requires the IP and MAC address(es) be static or reserved for the machine. If you have unused network interfaces that might draw or generate a random address, you will want to disable those interfaces before continuing.

You will find the latest server and examiner installation packages at https://www.f-response.com/support/downloads. In order to access this page you will need your license number (Ex. 1777x). In addition, server configuration is done via the Windows Configuration Console that is installed as part of the F-Response Universal Examiner windows installation package, regardless of whether the server is Windows or Linux.

Linux Specific Considerations

The F-Response Universal Server software is provided in RPM format for Centos/RedHat Enterprise Linux. The full scope of installing and configuring a Centos/RedHat Enterprise server is beyond the scope of this document, but the following should be considered specific to F-Response Collect.

Network Hardware and Licensing

Be sure to make sure all active network interfaces either have a static network address configured or are set to use DHCP with a defined reservation. This will greatly reduce the chances for license invalidation post install.

Firewall(s)

F-Response Universal is going to bind to and listen on TCP port(s) 80 and 443, as such, you will want to confirm there are no firewalls actively blocking traffic on that port. The proper configuration and management of firewalls is distribution specific and beyond the scope of this document.

Installing F-Response Universal

Note: All commands must be run with admin(root) privileges.

```
# rpm -Uvh F-Response-Universal-….rpm
```

Starting and Stopping F-Response Universal

Note: All commands must be run with admin(root) privileges.

```
# service fresuniv start
```

```
# service fresuniv stop
```

```
# service fresuniv status
```

Windows Specific Considerations

Your Windows server may be running one or both virtual adapter interfaces. We have found these interfaces often obtain or generate new addressing on reboot and are rarely used. Both should be disabled before installing the F-Response Universal Server. To disable, open an administrator command prompt and issue the following commands:

> "netsh interface isatap set state disabled"
> "netsh interface teredo set state disabled"

Download and run the **F-Response-Universal-Server-Installer-<versionnumber>.exe** for a Windows computer to begin the installation. If your server is Windows 10 or Windows Server 2019 or greater, you will want to set the newly installed "fresuniv" service start to "Automatic(Delayed Start)" under Properties->Startup Type.

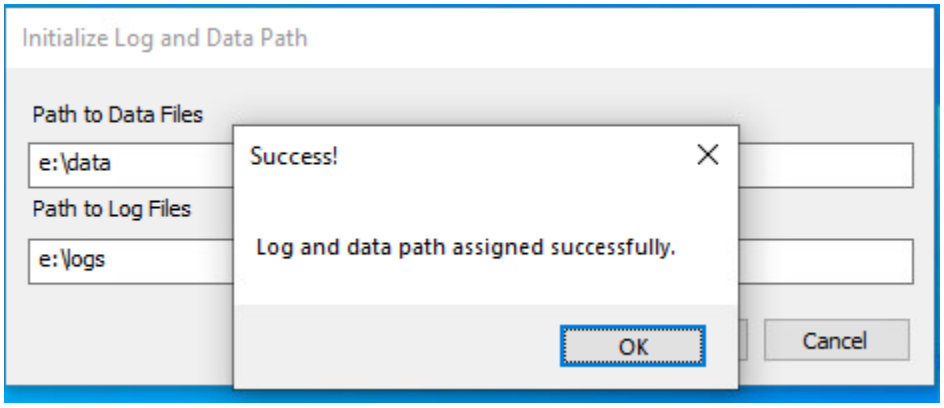
Initial Setup

All configuration of the F-Response Universal Server is done through the F-Response Configuration Console (console_configuration.exe). This tool is installed via the F-Response Universal Examiner installation package.

The first step after executing the tool is to input either the hostname or IP address of the remote Universal Server. Since this is a new and unconfigured server, the Configuration Console will step through a series of dialogs to configure the server for use.

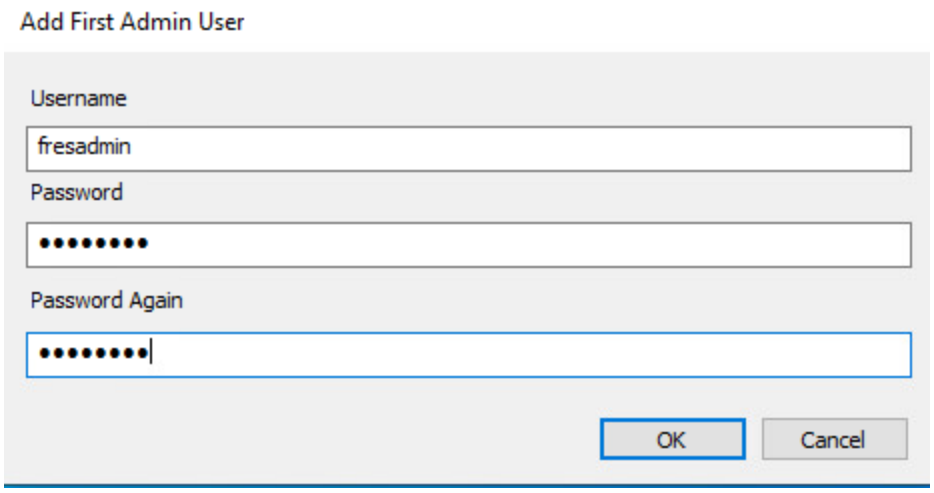
The first dialog will only appear on a Windows server installation. It will ask where you would like to save the log files and internal operative data files for F-Response Universal. These data files are small and contain user credentials as well as select application specific records. These data files DO NOT contain evidentiary data or subject data of any kind.

Make sure you provide data and log directories that would be outside of the installation path, as you will want the Universal server installation folder to be easily upgradeable going forward. In the example, we selected e:\data and e:\logs, however your specific selections will most certainly be different.

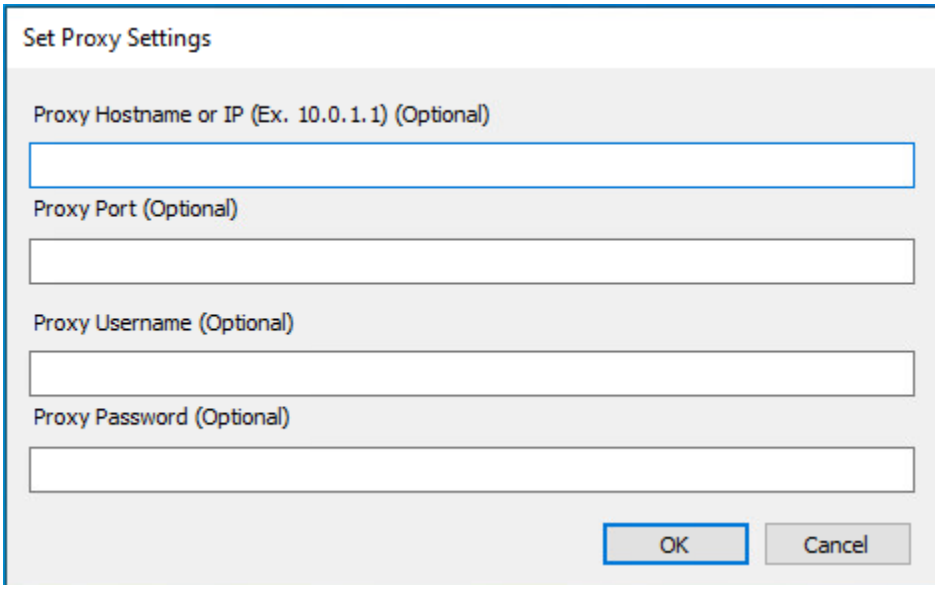


After the initial log and data path has been set, you will need to create the first administrative user. The dialog will prompt you to provide a username and password, as well as a confirmation password to ensure accuracy.

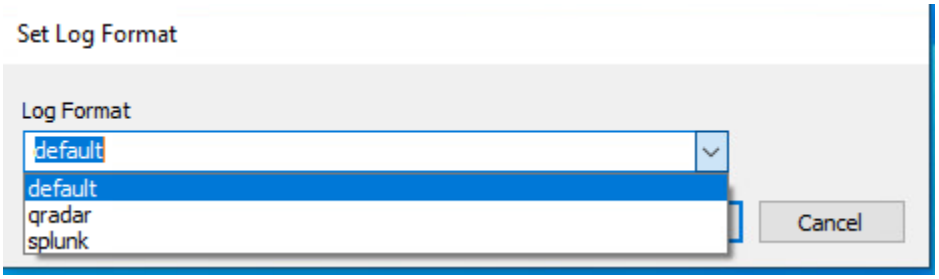
This is the user account can be used to login to both the Configuration Console and the F-Response Universal Management Console. It may be removed or changed later.



Once a valid account has been created, you will be prompted to input a proxy configuration (optional). This is necessary if your environment blocks the F-Response Universal server from accessing our internet facing licensing server(https://license.f-response.com) directly. If you do not need to input proxy information, leave these fields blank and click the **OK** button.

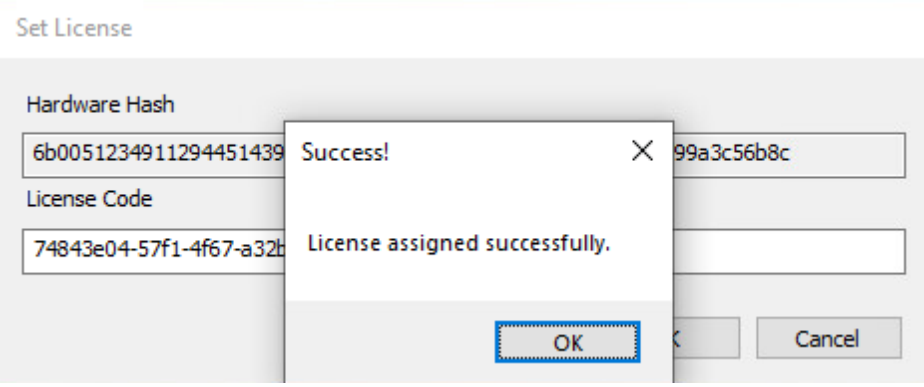


Next, you will be asked what format you would like for log records. Please select the most appropriate format for your environment from the available drop-down options.



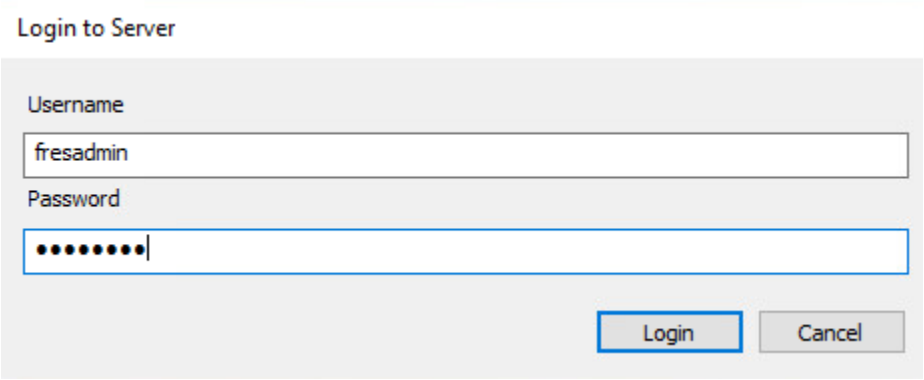
Logs will be stored in the location chosen earlier. This location can be changed later through the dashboard if necessary.

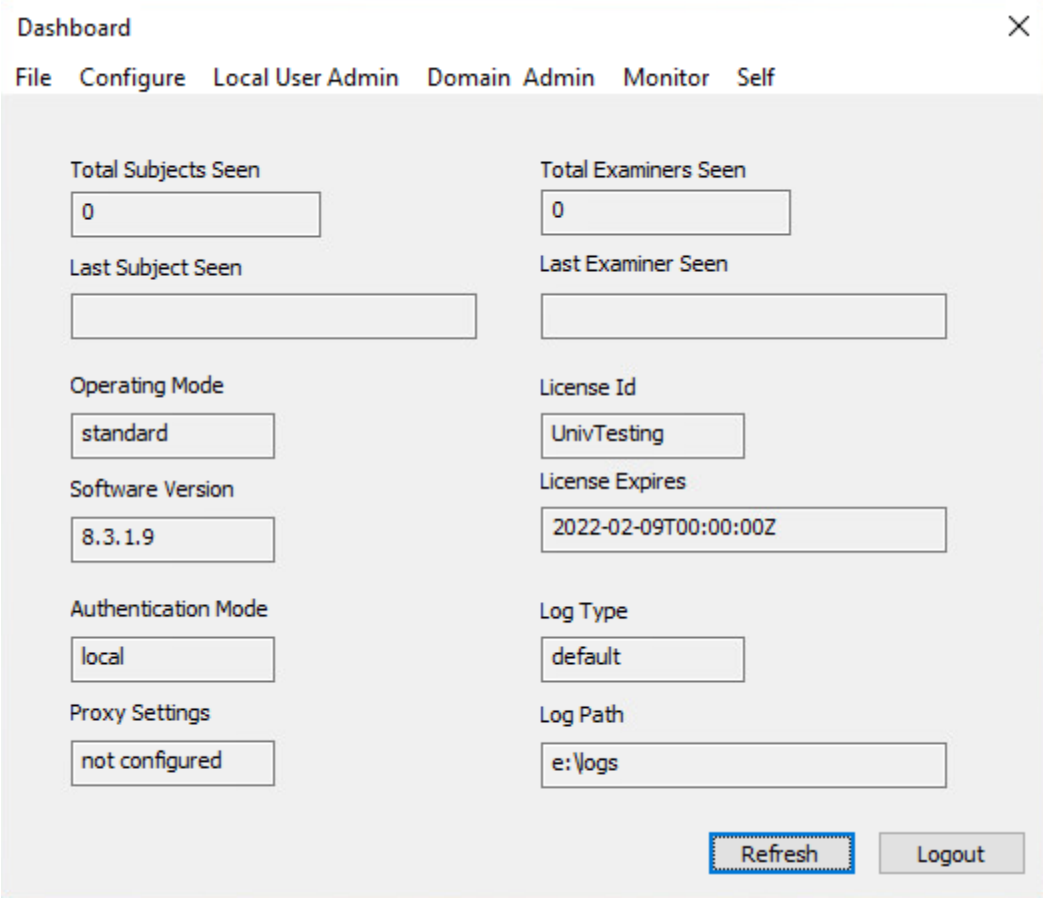
The next configuration item you will be prompted for is the license code as provided by F-Response. Do not share this code and be sure to save it in a secure location going forward. This code will be necessary should you ever need to reactivate your F-Response Universal server.



The hardware hash provided is a value generated by the Universal server based on the unique hardware configuration and should not be altered unless requested to by support. Paste in the license code and click OK to receive confirmation.

Provided everything worked correctly, you should be greeted by an F-Response Universal login screen. Please use the initial admin account created a few screens prior to login to the Server.



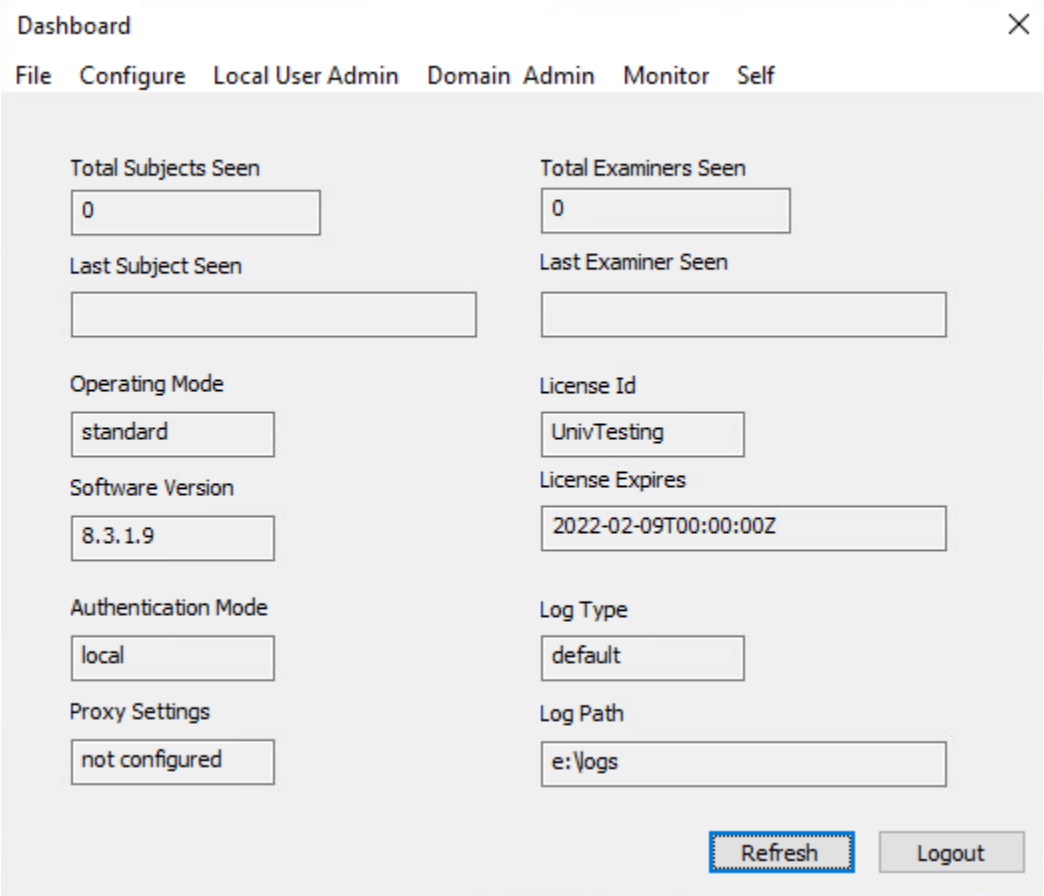


The F-Response Universal Dashboard provides you an overview of the current state of your F-Response Universal server. You will find each section highlighted in detail below.

Dashboard

Open the Configuration Console on your examiner computer and login with an administrator account.

Upon successful login you will be presented with your dashboard.



The dashboard provides an overview of your Universal server, specifically:

Total Subjects Seen: The total number of subject computers that have been connected to the server.

Total Examiners Seen: The total number of examiner (or administrator) computers that have been connected to the server.

Last Subject Seen: The hostname of the last subject computer to check in with the Universal Server.

Last Examiner Seen: The login of the last examiner to connect to the server using the management console.

Operating Mode: The Universal can be configured for standard (recommended), filtered, or mission mode.

License ID: The license number assigned to this server (needed for renewals and software downloads).

License Expires: The date the license for the server will expire. (If a renewal has been paid and processed this field will update to the new date automatically once the current license expires.)

Software Version: The software version number currently running on the server.

Log Type: The current logging format (default is CSV).

Authentication Mode: Authentication mode for the server can be set for Active Directory or local authentication.

Log Path: The location on the server where the logs are stored.

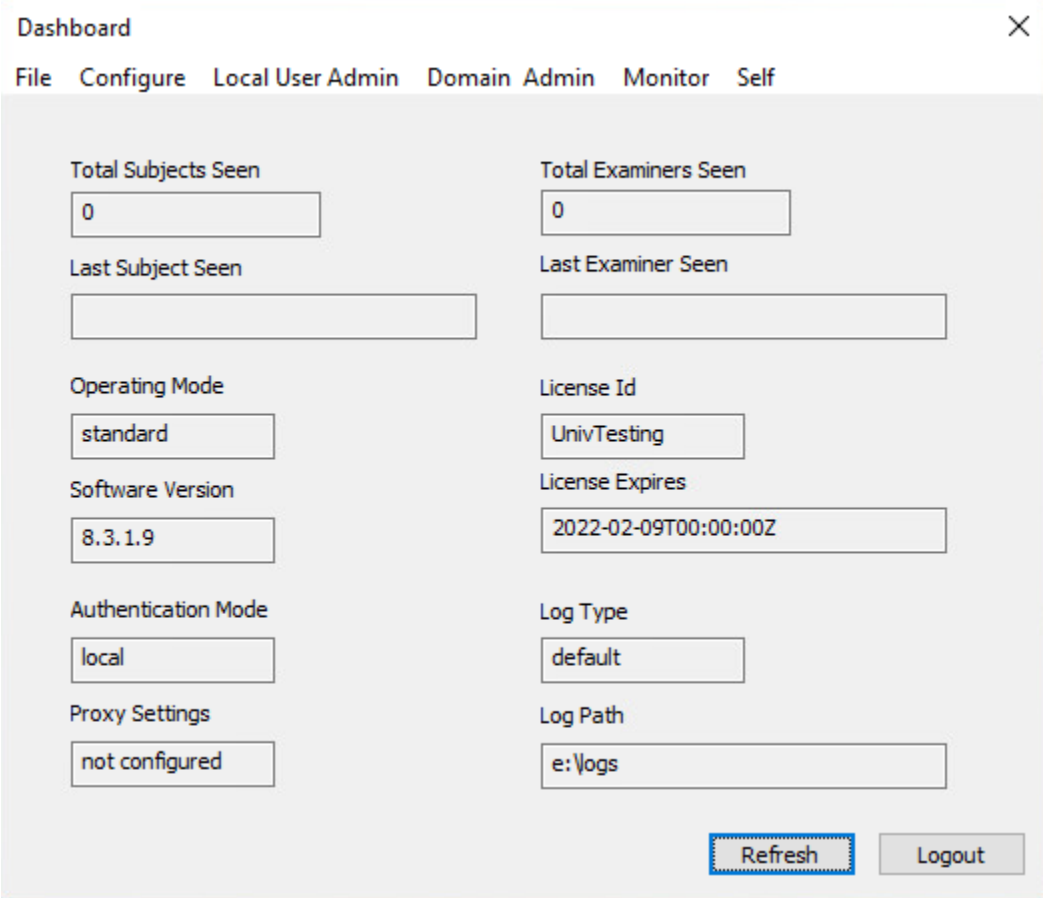
Proxy Settings: This field specifies if the server is configured to use a proxy for access to the F-Response licensing server.

Each of these fields are explained in further detail in their respective section below.

Licensing/Software Updates

Open the Configuration Console on your examiner computer and login with an administrator account.

Upon successful login you will be presented with your dashboard.



There are three important fields here to note for software and licensing: **Software Version, License Id,** and **License Expires**.

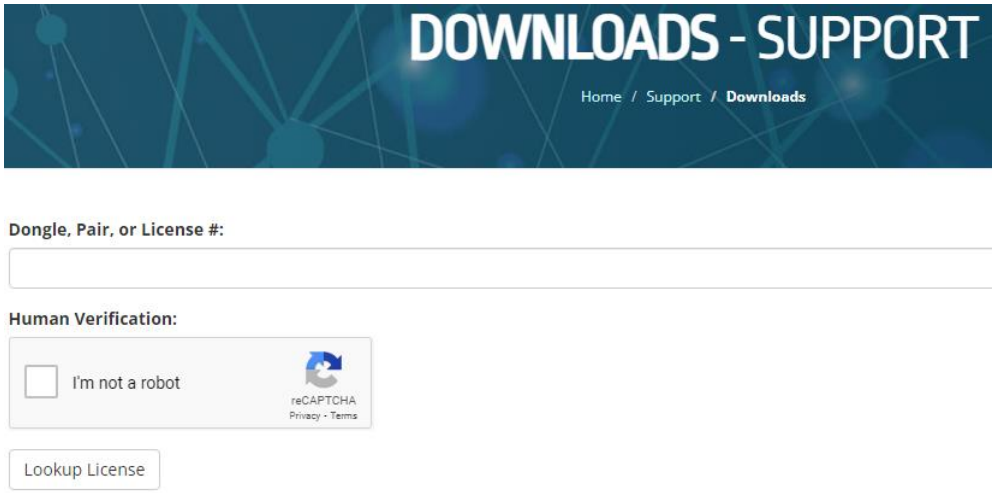
Software Version Number

The **Software Version** number of the Universal Server software you are running is provided on the Dashboard. Please make sure you are running the latest version of the software. There is no cost to upgrade to the latest version provided your license is not expired.

The latest version of the software is always available from the download section of the F-Response website https://www.f-response.com/support/downloads. You will need your license ID number (below) to access the downloads.

License ID

The License ID number for your Universal server is provided on the Dashboard. This number can be entered into the downloads page https://www.f-response.com/support/downloads on the website to check for and obtain the latest version:



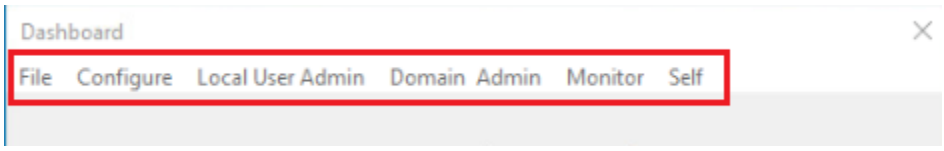
License Expiration

F-Response Universal is sold in 1- and 3-year license terms. The Universal software will cease to function on the expiration date shown on the dashboard. To renew F-Response Universal at the discounted renewal rate, the purchase must be made within 30 days post expiration.

To renew, go to the software renewals page on the F-Response website https://www.f-response.com/buyfresponse/software-renewals and complete the checkout process. Once the renewal is processed and the current license reaches expiration, the new license will automatically be downloaded and updated on the server.

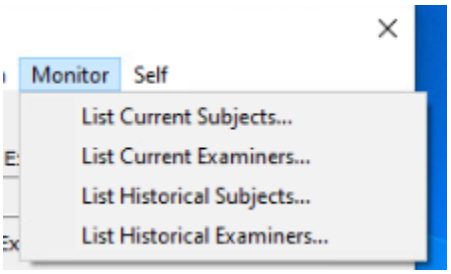
Server Administration

The Universal server can be configured using the drop-down menus along the top of the window.



History

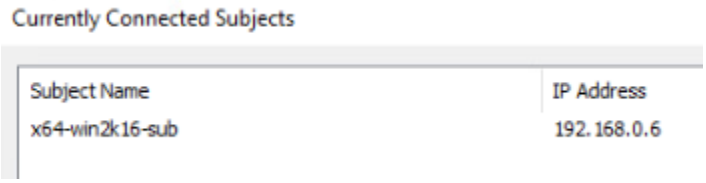
Access to the history details on your server can be found by clicking on the **Monitor** drop-down menu option on the top of the window:



The drop-down menu gives you the option to view the examiners or subjects that are currently active and connected to the server or to view the historical data on the server (When an examiner or subject was last seen by the server). All the options for Subject and Examiner machines are covered in more detail below.

Subjects

To view the Subject computers currently active and connected to the Universal server, choose **List Current Subjects…** from the **Monitor** drop-down menu on the dashboard.



Simply click the **OK** button when you have completed your review of the data.

To view the history of all the subject computers that have connected to the Universal server you can choose **List Historical Subjects…** from the **Monitor** menu on the dashboard.

Subject History

Hostname	IP Address	Last Seen
X64-WIN81-SUB	23.1[redacted]	2023-05-10T14:21:42Z
X64-WIN10-SUBDE	23.1[redacted]	2023-10-16T19:38:29Z
X64-WIN10-SUB	23.1[redacted]	2023-10-16T19:37:48Z
X86-WIN10-SUB	23.1[redacted]	2023-02-21T04:36:20Z
X64-WIN7PRO-SUB	23.1[redacted]	2021-03-19T14:23:09Z
X64-WIN11-SUB	23.1[redacted]	2023-10-16T19:38:29Z
X64-LINUX-SUB-RL9.FRESPONSE.L...	23.1[redacted]	2023-09-06T00:06:03Z
X64-2K12R2-SUB	23.1[redacted]	2021-03-31T15:53:13Z
EC2AMAZ-H5N9RPQ	52.8[redacted]	2021-06-05T22:34:38Z

Export | Delete All | Refresh | Exit

Here you can see the hostname and IP address of the subject, and the last time it checked in with the server. You can also sort on any of the 3 columns depending on what you are looking for in the data. There is also an option to export the subject history to a csv file by clicking the Export button.

Lastly, you may choose to clear the Subject History completely. It is important to note this operation cannot be undone. After clearing, a new historical database will repopulate as subjects check-in with the server. To clear the subject history, click the **Delete All** button.

Examiners

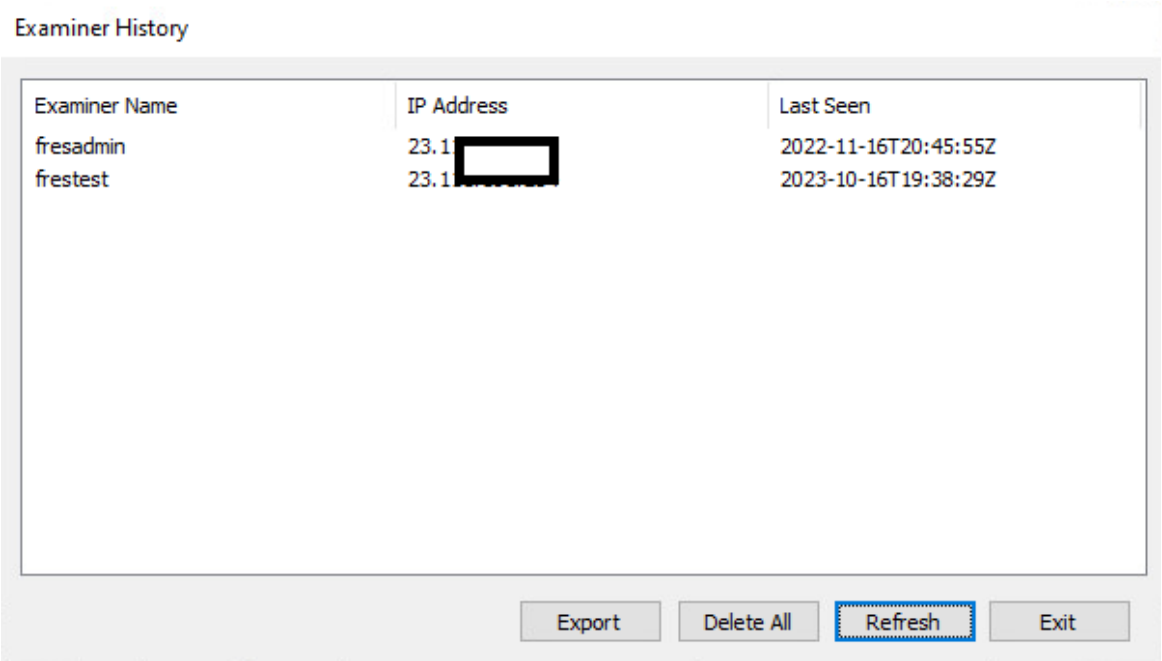
To view the examiners and administrators currently connected to the Universal server, choose **List Current Examiners…** from the **Monitor** drop-down menu on the dashboard.

Currently Connected Examiners

Examiner Name	IP Address
frestest	192.168.0.38

Simply click the OK button when you have completed your review of the data.

Choose **List Historical Examiners…** from the **Monitor** menu on the dashboard to view examiner computers that have checked into the server.

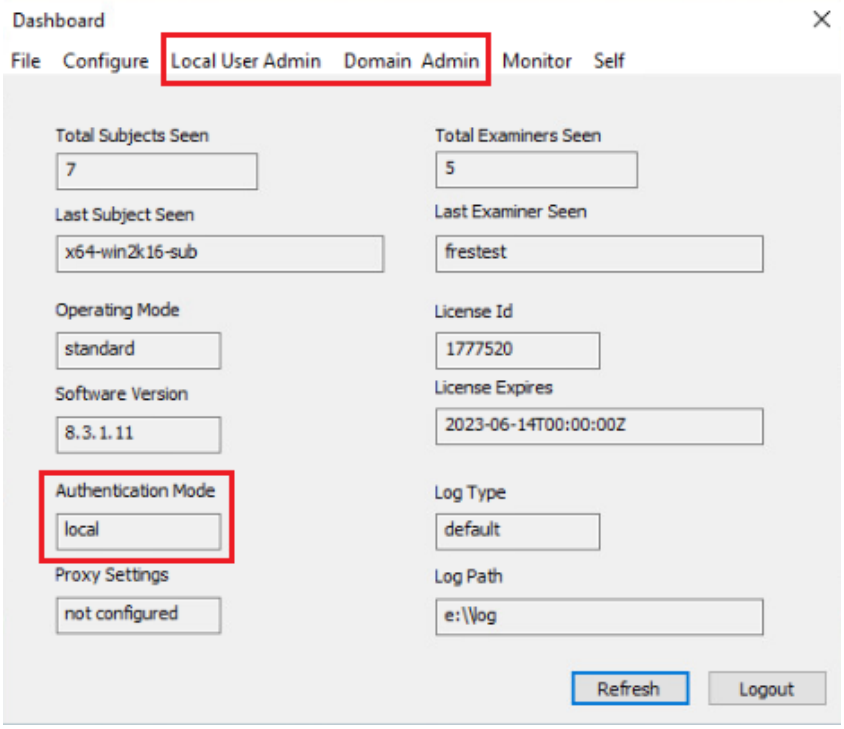


Here you can see the examiner name, IP address of the examiner computer, and the last time the examiner logged into the server using the console. You can also sort on any of the 3 columns depending on what you are looking for in the data. There is also an option to export the examiner history to a csv file by clicking the Export button.

Lastly, you may choose to clear the Examiner History completely. It is important to note this operation cannot be undone. After clearing, a new historical database will repopulate as examiners login to the server using the management console. To clear the examiner history, click the **Delete All** button.

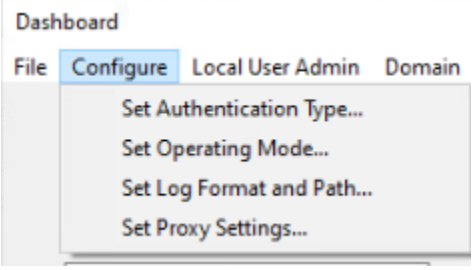
Authentication

The current **Authentication Mode** is visible on the Dashboard.



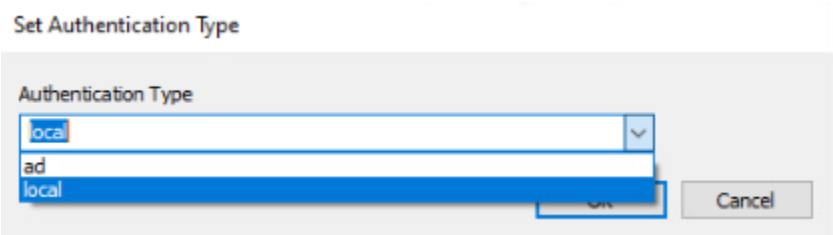
Authentication Mode

The F-Response Universal server can be set to **Local** or **Active Directory** Authentication.



Choose **Set Authentication Type…** from the Configure drop-down menu.

Then choose the Auth Type from the dropdown:

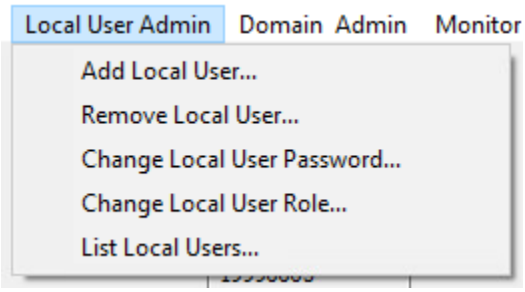


And click the OK button to set the server in the authentication mode needed.

Additional management for Local Users or Active Directory settings are covered in those sections of this manual.

Managing Local User Accounts

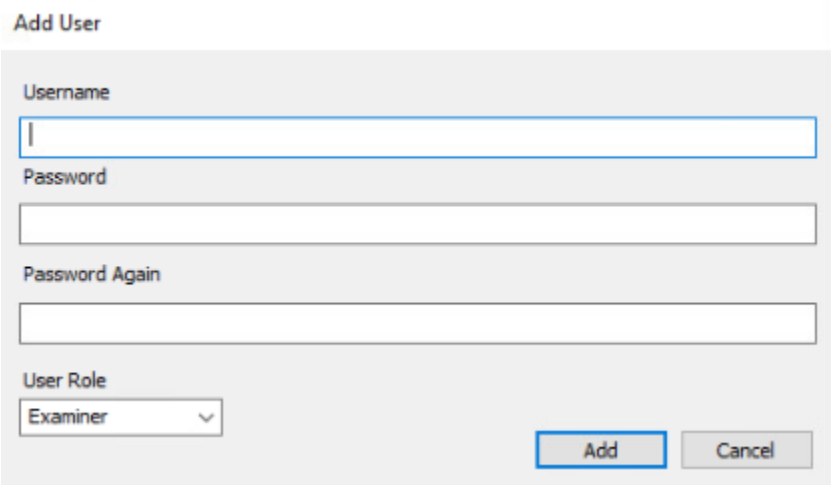
Local Accounts on the Universal server can be configured from the Dashboard under the **Local User Admin** drop down menu. **Note: Local accounts are only used if Active Directory Authentication is not enabled.**



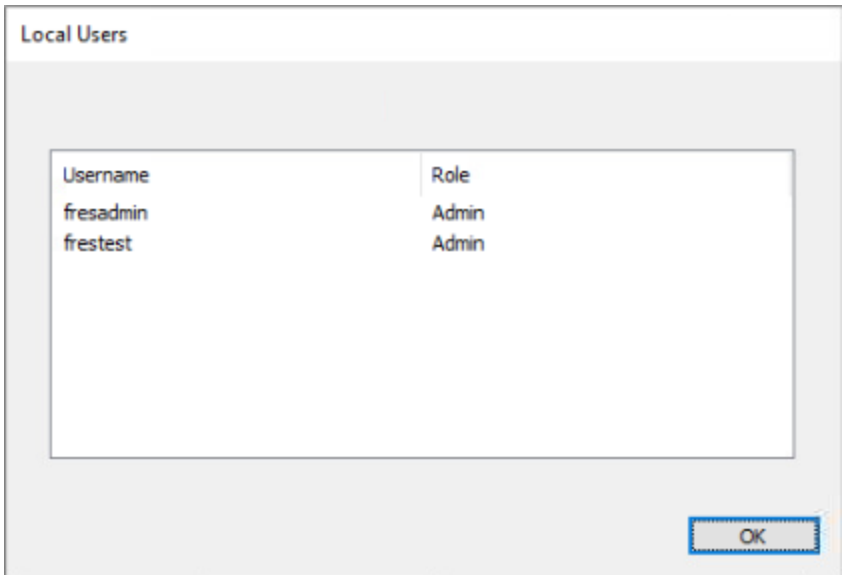
Details of each menu option are covered below.

Add a local user account

Click the **Add Local User…** option from the drop-down under the Local User Admin menu on the Dashboard to add a new examiner or Universal administrator to the Universal server.

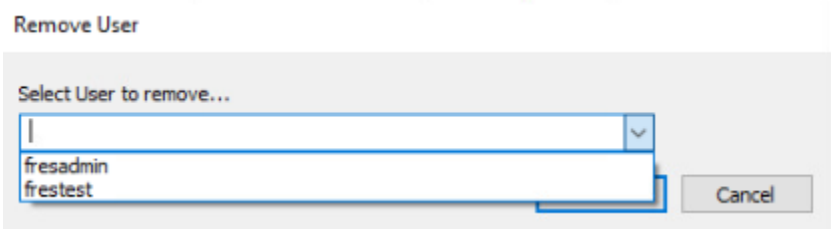


Simply enter the details and role information and click the **Add** button. The new user and their assigned role will appear in the **List Local Users…** option from the **Local User Admin** drop down menu.



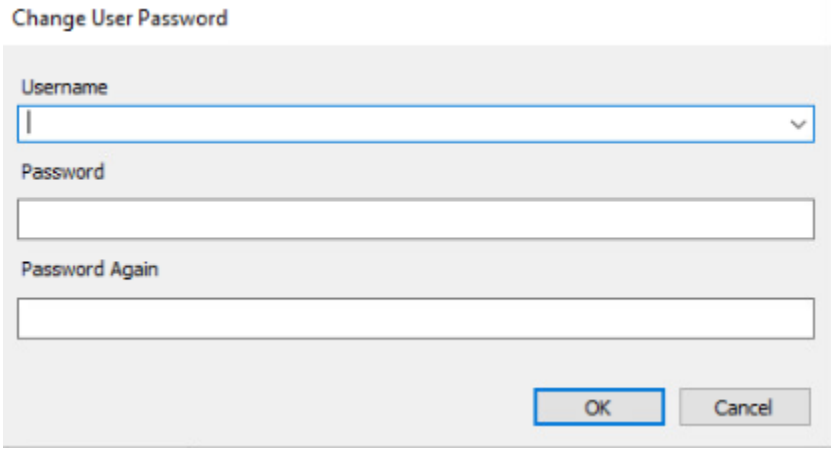
Remove a local user account

To remove a local user account from the server, select the **Remove User…** from the **Local User Admin** drop-down menu, then select the User from the drop-down list and click the **Remove** button.



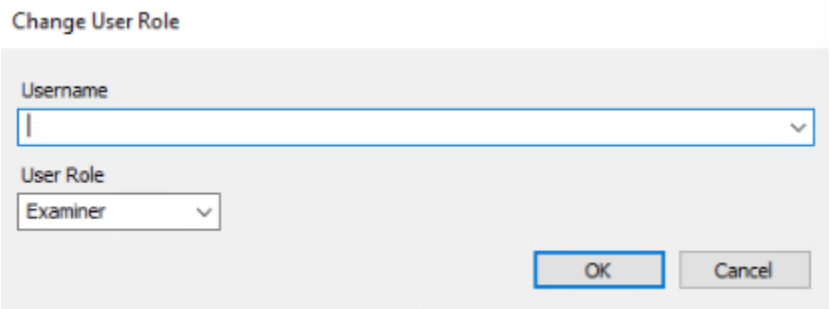
Changing a local user password

To change the password for a local user account, select the **Change User Password…** option from the **Local User Admin** drop-down menu. Select the appropriate user account and enter the new password, then confirm by clicking the **OK** button.



Changing a local user role

To change the role for a local user account, select **Change User Role…** from the **Local User Admin** drop-down menu. Here you can select the User from the drop-down list and choose the role (*Examiner or Administrator).



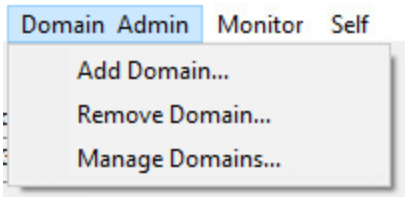
The **Examiner** role allows for full use of F-Response Universal capabilities using the F-Response Universal Management Console and view-only permissions of the F-Response Universal Server Dashboard via the F-Response Server Configuration Console (console_configuration.exe). If the Universal Server is configured for Mission Mode the examiner will only see missions they have created in the management console.

The **Administrator** role allows for full use of F-Response Universal capabilities using the F-Response Universal Management Console and full management of the F-Response Universal Server via the F-Response Server Configuration Tool (console_configuration.exe). If the Universal Server is configured for Mission Mode an Administrator will see all missions created themselves and by other examiners/administrators in the management console.

Active Directory Domain Configuration

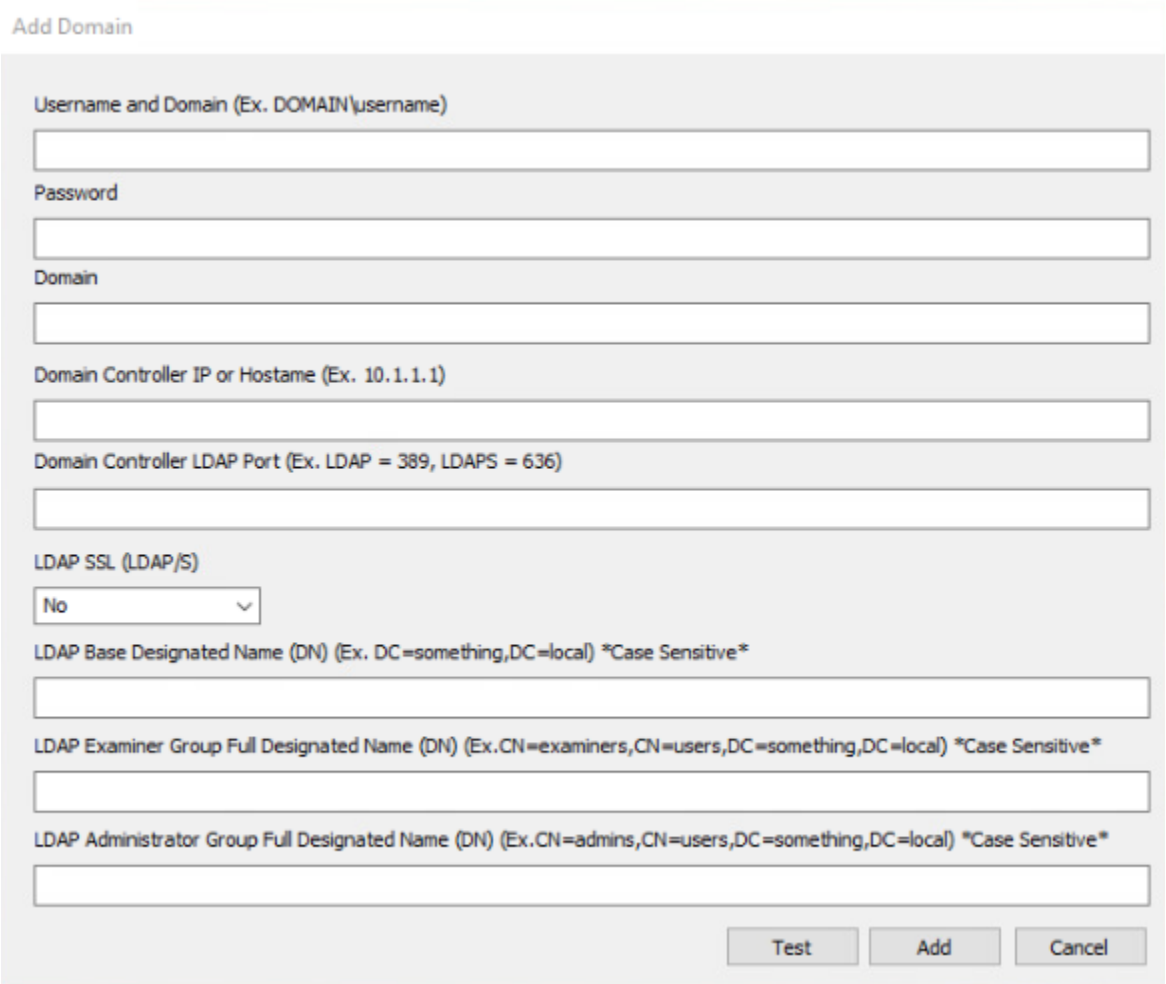
Adding your Active Directory domain

With Active Directory (LDAP) authentication enabled, local user accounts will no longer reside on the F-Response Universal server itself, rather the server will be configured to authenticate users directly against Active Directory based on group membership.



To configure the server with your Active Directory information, login to the dashboard and choose **Add Domain** from the Domain Admin drop down menu.

This will open the Add an Active Directory Authentication Domain window as pictured below.



Notice each field contains tips for how the data should be formatted. Once all the data is entered you can test everything is correct by clicking the **Test** button before committing by clicking the **Add** button.

- Username and Domain
  - A valid Active Directory account.
- Password
  - A valid Active Directory account password.
- Domain

    - Active Directory Domain you wish to add—must be the same one used for the Username and Domain above.
- Domain Controller IP or FQDN
    - The IP address or the Fully Qualified Domain Name of the Domain Controller (DC).
- Domain Controller LDAP Port
    - The TCP Port number LDAP runs on in your environment.
- LDAPS(With SSL Enabled)
    - If using LDAPS with SSL enabled select Yes from the drop-down.

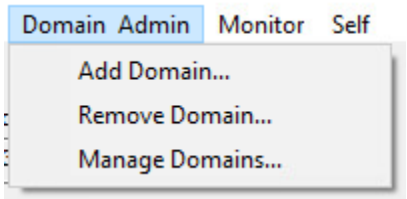
To configure F-Response Universal for Active Directory Authentication you will need two groups, one for Administrators and another for Examiners, along with the full LDAP name for each group. **Note: F-Response Universal does not support nested groups.**

- LDAP Base Designated Name (Case Sensitive, no spaces between commas)
    - The base name for the Active Directory Domain.
        - Ex. "DC=fresponse,DC=local"
- LDAP Admin Group Full Designated Name (Case Sensitive, no spaces between commas)
    - The full name for the Active Directory Domain group that contains F-Response Universal administrator users.
        - Ex. "CN=universaladmins,CN=Users,DC=fresponse,DC=local"
- LDAP Examiner Group Full Designated Name (Case Sensitive, no spaces between commas)
    - The full name for the Active Directory Domain group that contains F-Response Universal examiner users.
        - Ex. "CN=universalusers,CN=Users,DC=fresponse,DC=local"

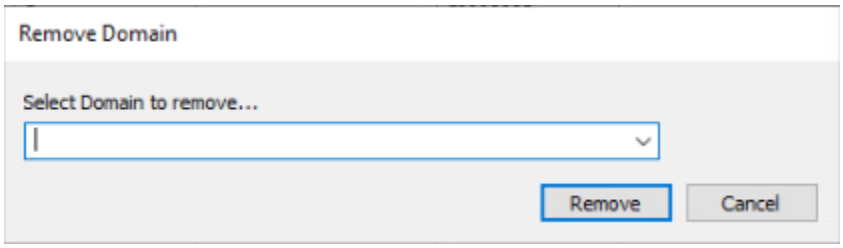
Note: Remember to set the Authentication Type to Active Directory to enable AD logins.

Removing your Active Directory Domain

To remove an active directory domain, login to the dashboard and choose **Remove Domain** from the Domain Admin drop-down menu.

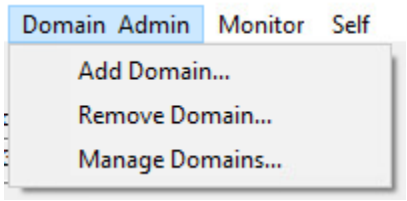


The Remove Active Directory Authentication Domain window will appear, simply choose the domain you wish to remove from the drop-down list and click the **Remove** button.

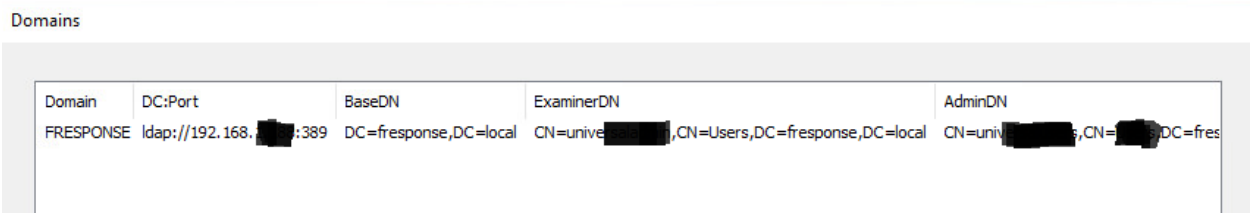


Manage Domains

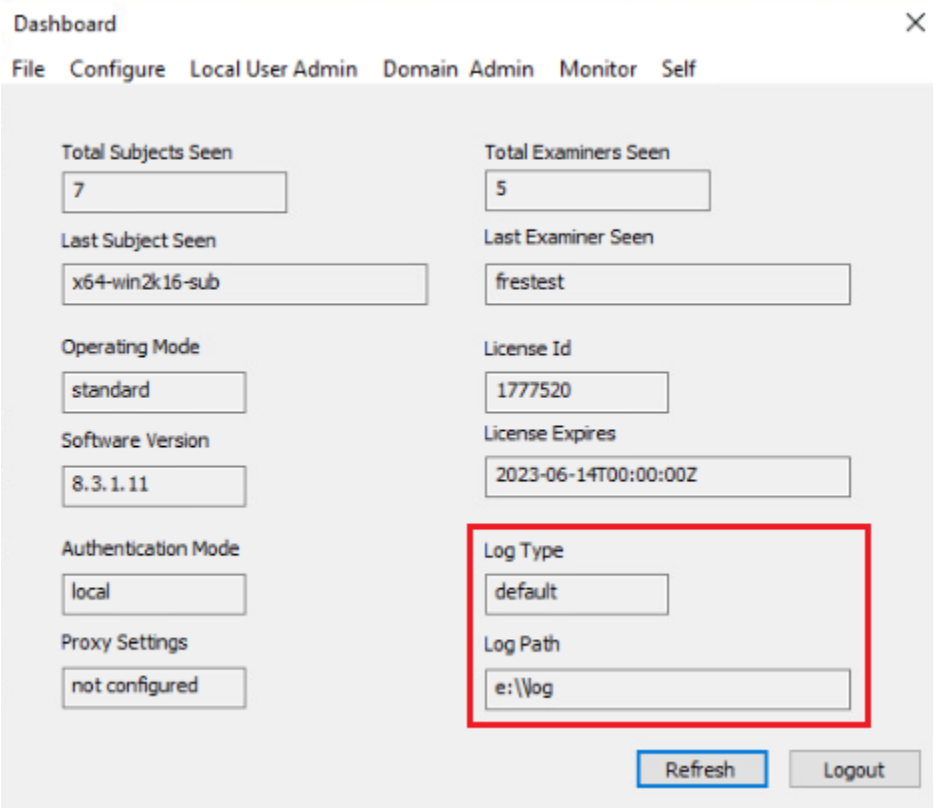
To view the currently configured active directory domains, login to the dashboard and choose **Manage Domains…** from the Domain Admin drop-down menu.



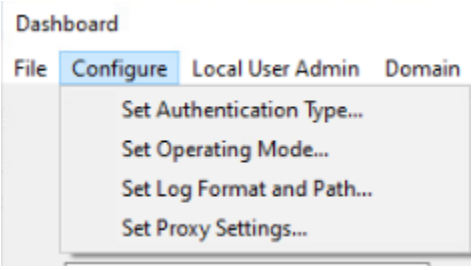
The Domains window will appear with all configuration details for each domain.



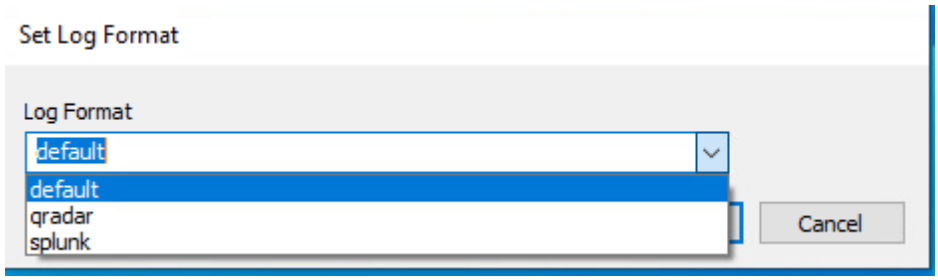
Logging



By default, the F-Response Universal Server will store logs in CSV format in either the provided logs directory (Windows) or "/var/fresuniv/logs" (Linux). The server also offers the option to store logs in QRadar or Splunk format if needed.



To modify the log format or location, choose **Set Log Format and Path…** from the **Configure** drop-down menu on the Dashboard. This will allow you to choose the desired log format from the drop-down list. Select the required log type, modify or verify the Log Destination, and click OK.



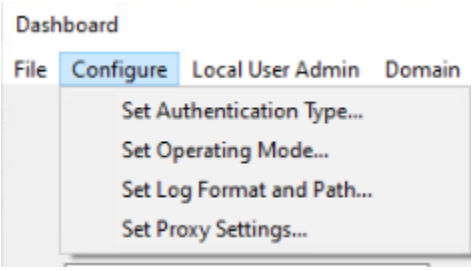
All F-Response Universal log entries share the same values:

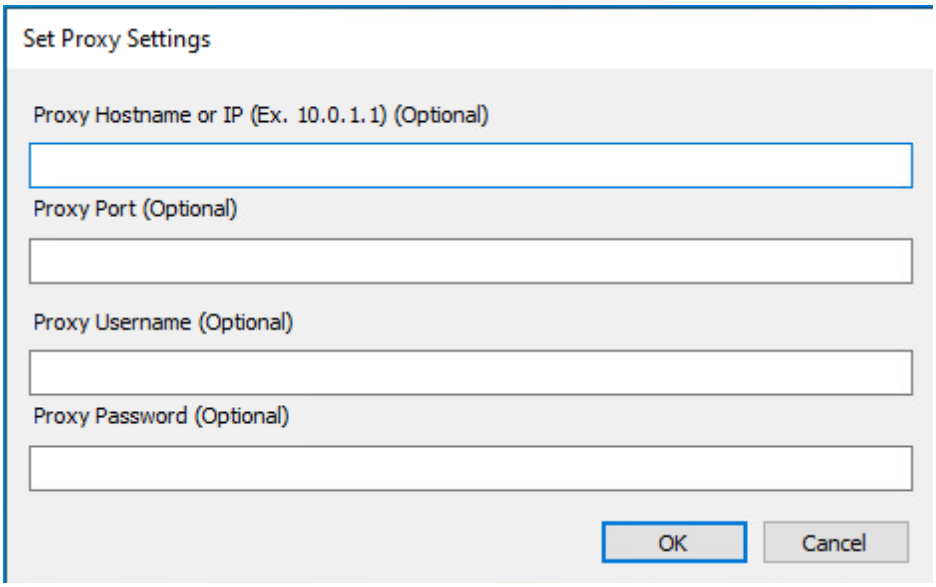
- Function:
  - Name of the subsystem involved.
- Username:
  - Where possible, includes the user, subject, or IP matching the event.
- Datetime:
  - Date and time when the event took place in UTC.
- Type:
  - Informational (info) or Error (error).
- Message:
  - Text based details.

For complete details on Log Formats, please see Log Formats in Appendix D

Proxy Settings

The Universal server can be configured to use a web proxy for accessing https://license.f-response.com under the **Configure** drop-down menu option from the Dashboard. Choose **Set Proxy Settings…** to open the configuration window.





Here you can enter your proxy information (or clear the fields to remove the proxy) and click **OK** to confirm.

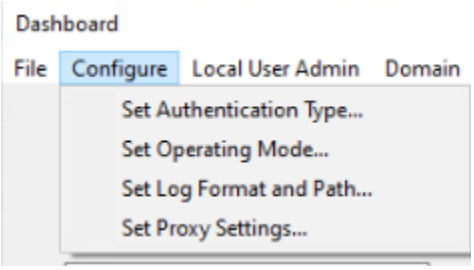
Operating Mode

The Universal server can be set to run in one of 3 different modes, changing the operation mode will require a restart of the Universal server service to take effect.

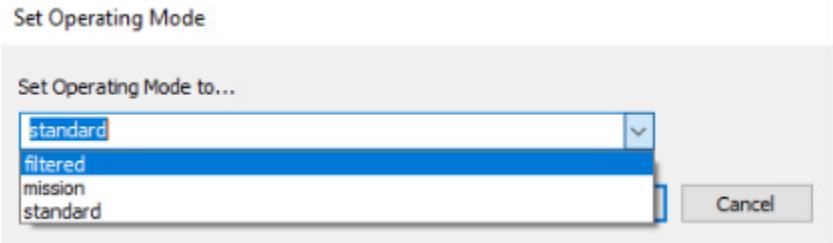
Standard mode: If F-Response is deployed on an as-needed basis ***(recommended method)***, the server should be set to run in Standard mode.

Filtered mode: If F-Response is deployed and running across the enterprise, the server needs to be set in Filtered or Mission mode to manage the number of subjects that appear in the console. Filtered mode will instruct subjects to disconnect in the event their hostname does not match the configured filter string.

Mission mode: Can be enabled for tighter controls and segregation of duties. When Mission mode is enabled, examiners must create a mission and add the machines they wish to view. Examiners will then see the machines as they connect and perform their assigned tasks. Each mission is specific to the examiner and examiners will not see machines tasked to another examiner's mission. Admins can view and manage all the created missions in the system.



Change the operating mode by clicking **Set Operating Mode…** from the **Configure** drop-down menu. This will open the **Set Operating Mode** window where you can choose your operating mode:

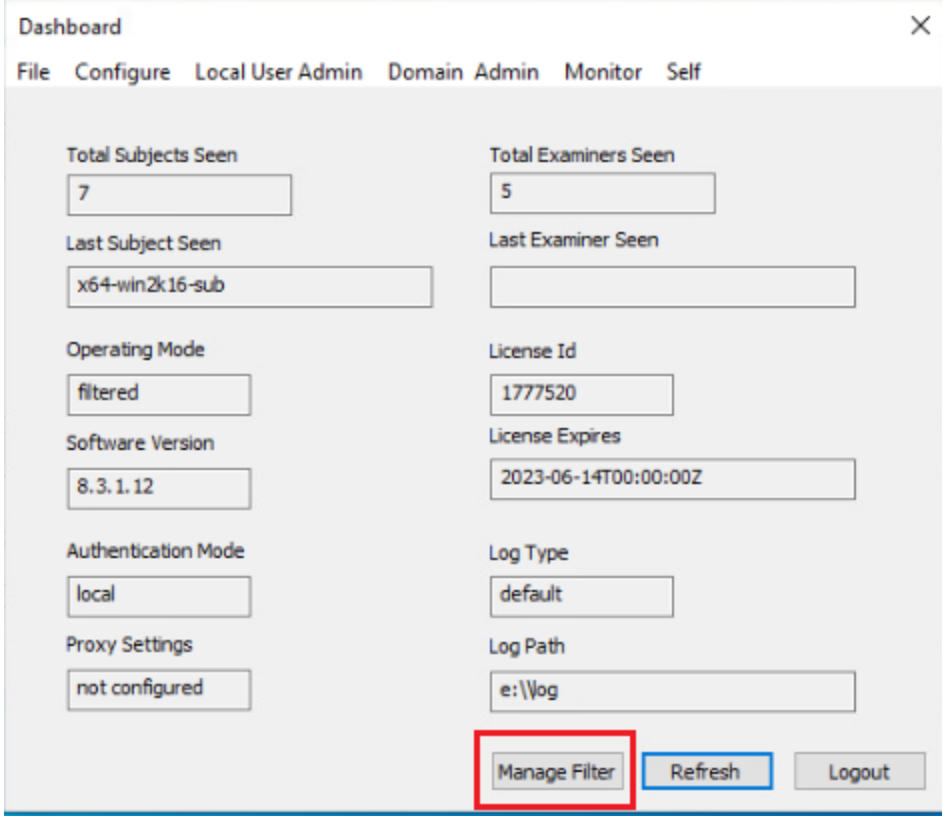


Choose the preferred setting from the dropdown and click the **OK** button.

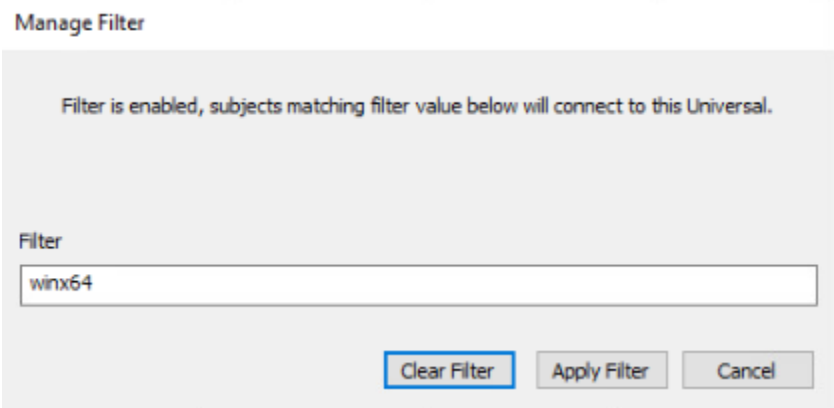
Filtered Mode

If F-Response is pre-deployed across the environment via MSI using your software management tools (such as SCCM), Filtered mode can be enabled to manage the number of subjects that appear in the console at any given time.

Once Filter mode is set, there will be an additional button labeled **Manage Filter** added to the dashboard (click Refresh if you do not see the button after changing the mode).



In the Manage Filter window, you have the option to apply a new filter, or clear the current filter. Note if there is no filter set, no subject computers will appear in the console.



Once a filter is set, it will take time for any matches to appear in the Universal Examiner console(s). The length of time is dependent upon the wait hint set when the software was deployed (default is 3600 seconds, or 1 hour). Subjects will check in at the predetermined wait hint interval to see if they match a filter and will connect to the server when a match is confirmed.

Please note, filters are text based. They only apply to the subject's hostname. In the above example, any subject with winx64 in the hostname would be considered valid and be allowed to connect.

Mission Mode

Mission mode can be used with an as-needed or pre-deployment model. If Mission mode is enabled examiners must create missions and add the subject machine(s) they wish to see in the console. Examiners cannot see machines assigned to another examiner's mission and a machine can only belong to one mission at a time. Examiners can manage only missions they have created. Admins can manage all missions in the system. Further details on the mission system can be found here.

Additional Options

IPv4 Restrictions

Customers looking to apply additional access controls to their Universal server can use the following addition to the fresuniv.cfg file to restrict examiner access to select IP addresses. Examiners will still have to login.

IP addresses must be provided in the following format, individual addresses, or ranges. See examples below:

"iprestrictions":["IP1","IP/NET","IP3"]

Ex. "iprestrictions":["192.168.2.1","172.16.10.0/24", "10.0.1.2"]

Changing Listening Port(s)

Customers looking to alter the listening ports from the default (80, 443) can do so they adding the following values to the fresuniv.cfg file and restarting the F-Response Universal service/server:

"adminport":XXX

"port":XXX

Ex. "adminport":4433,"port":8080

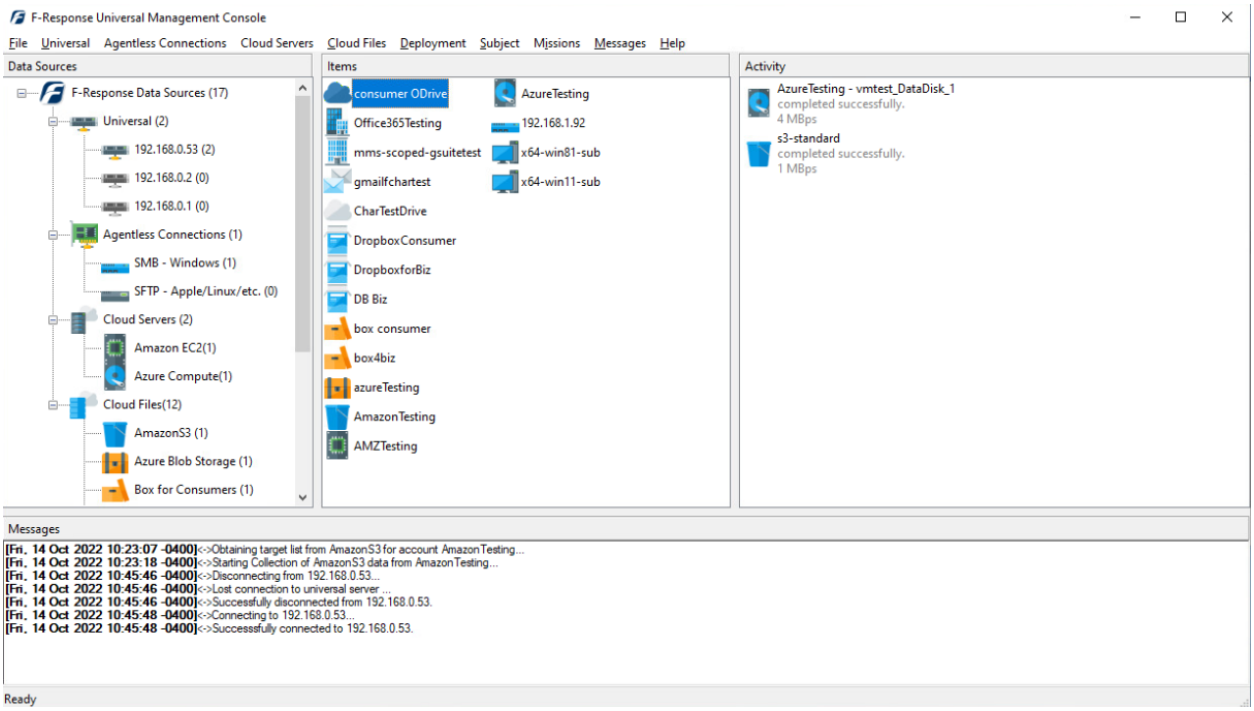
Getting started with the F-Response Management Console (Windows)

Installation

Download and run the **F-Response-Universal-Examiner-Installer-<versionnumber>.exe** for a Windows computer from the F-Response Website: https://f-response.com/support/downloads

Note: You will need your license number to download the software. (Ex: 1777x)

Overview



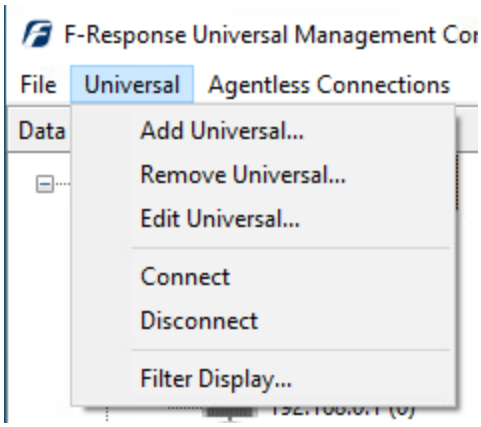
The F-Response Universal Management Console operates with a left to right workflow. The various Data Sources appear in the left column, Items to interact with appear in the center column, and connected disks and operations appear in the rightmost column.

F-Response provides connectivity to resources on remote machines, as well as full imaging capability of logical volumes and physical disks on those remote machines. For targeted collection of a subset data on a remote computer, any third party forensic tool that works with a locally attached disk will work with an F-Response connected disk. F-Response is vendor neutral and will work with any number of Forensic/eDiscovery/IR tools that can interact with a locally attached write-protected disk.

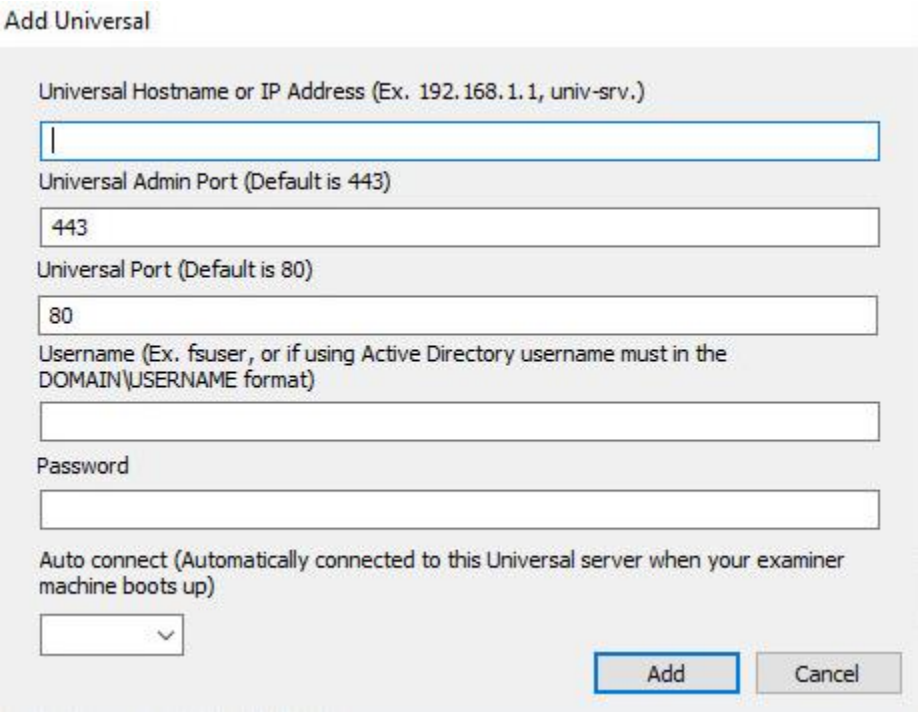
F-Response provides full and direct collection capability from a number of different cloud providers and, in the case of most business class accounts, can enumerate custodians using an administrator account.

Adding a Universal Server

A Universal Server can be added to the F-Response Universal Management Console by choosing the **Universal** drop-down menu, and clicking on **Add Universal…**



This will open the Add Universal window.



These six fields are as follows:

Universal Hostname or IP address: Each Universal server must be entered individually, enter only one Universal server or IP address here.

Universal Admin Port: This field is populated with the default port 443 but can be reconfigured if necessary (change must be made on the server itself before adding here).

Universal Port: This field is populated with the default port 80 but can be reconfigured if necessary (change must be made on the server itself before adding here). All traffic on this port is AES-256

encrypted, it is recommended use the common port 80 for ease of communication with subject computers throughout the environment.

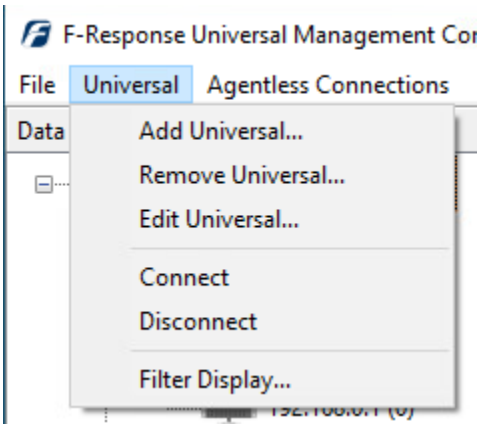
Username: The local or Active Directory user that has been assigned an Examiner role on the Universal server.

Password: The local or Active Directory account password.

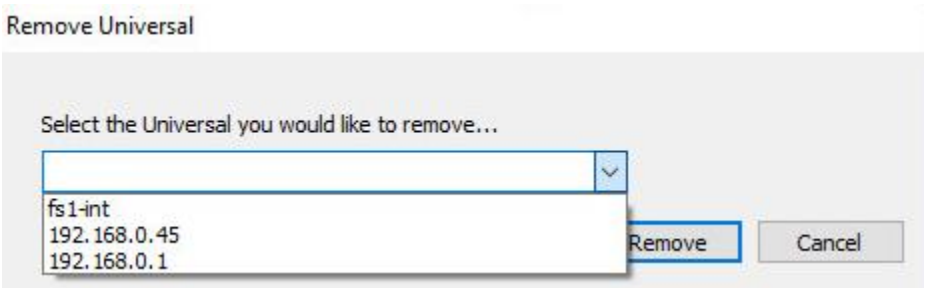
Auto connect: Choose Yes or No to connect automatically to the Universal server on startup.

Removing a Universal Server

A Universal Server can be removed from the F-Response Universal Management Console by choosing the Universal drop-down menu, and clicking on **Remove Universal…**

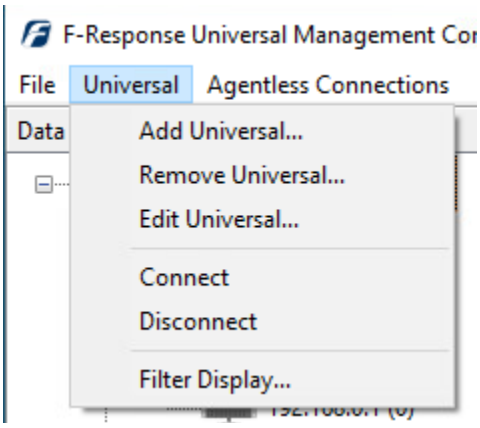


This will open the Remove Universal window where the Universal server to be removed can be selected from the drop-down list. Choose the server and click Remove to finalize.

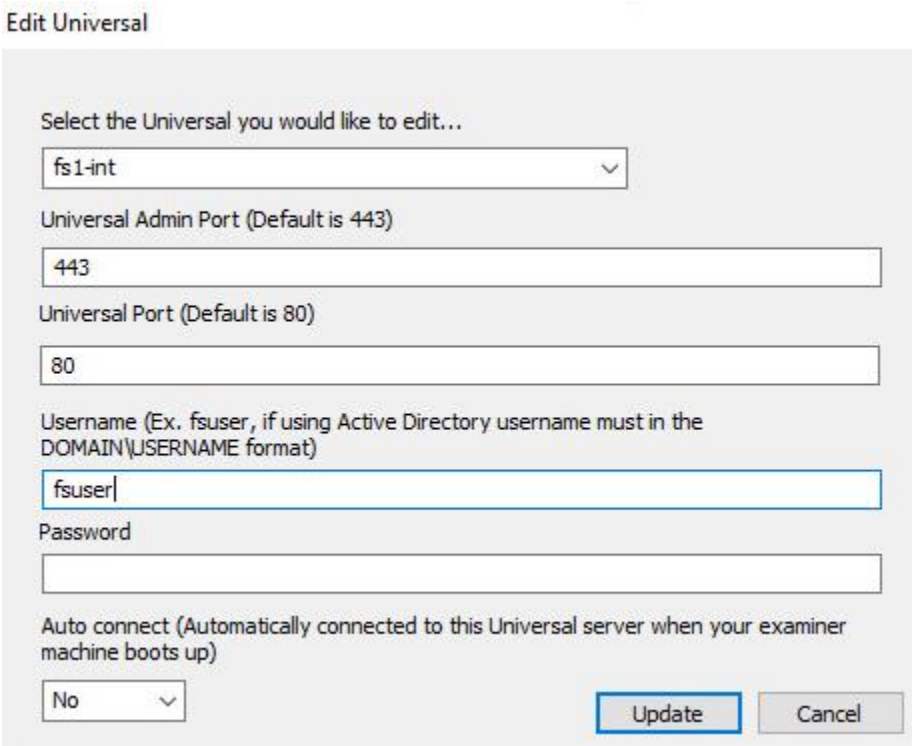


Edit a Universal Server

You can edit any of the existing fields for a Universal server in the console by simply choosing **Edit Universal…** from the **Universal** drop-down menu.



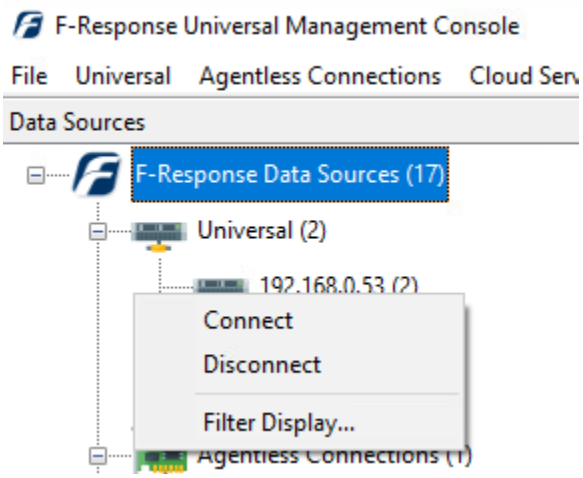
This will open the Edit Universal Window:



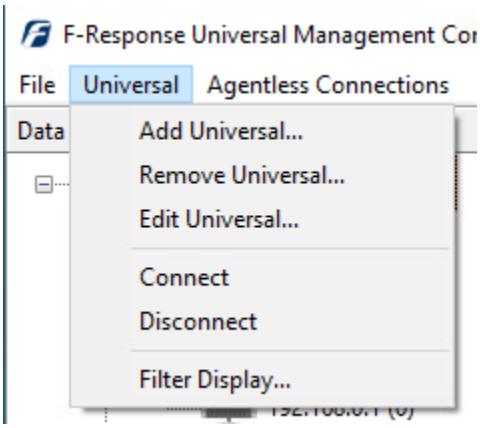
Choose the Universal server you would like to edit from the drop-down list then edit the appropriate fields. Click **Update** to confirm the changes.

Connecting or Disconnecting from a Universal Server

To connect or disconnect from a Universal server in the F-Response Universal Management Console, simply highlight the Universal server under the **F-Response Data Sources** in the left column, then right click and choose to **Connect** or **Disconnect**:

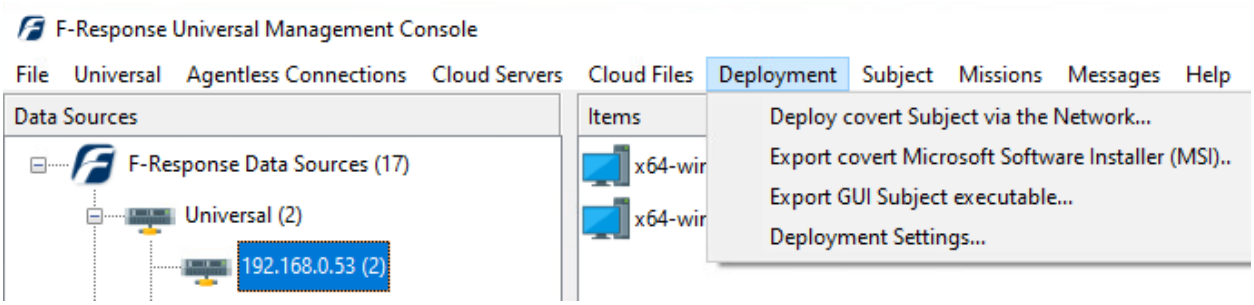


Alternatively, highlight the Universal server then choose **Connect** or **Disconnect** from the **Universal** drop-down menu:



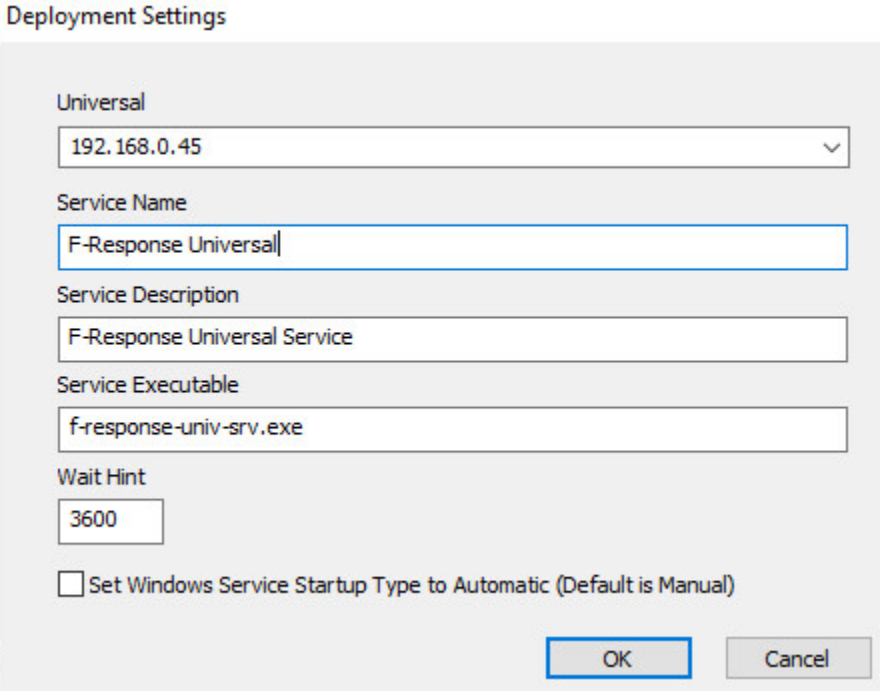
Deployment

F-Response Universal can be deployed to remote subject computers in the environment covertly from the Console, via MSI, or by a GUI executable. All these options are covered below.



Deployment Settings

Default deployment settings can be accessed and modified under **Deployment** -> **Deployment Settings…**



These fields are as follows:

Universal: Choose the Universal server you wish you modify the deployment settings for from the Universal drop-down box.

Service Name: Universal runs as a service on the remote subject computer, create a service name that does not conflict with an existing service.

Service Description: Description value that will be assigned to the F-Response subject service when installed on the remote computer(s). This description is completely optional.

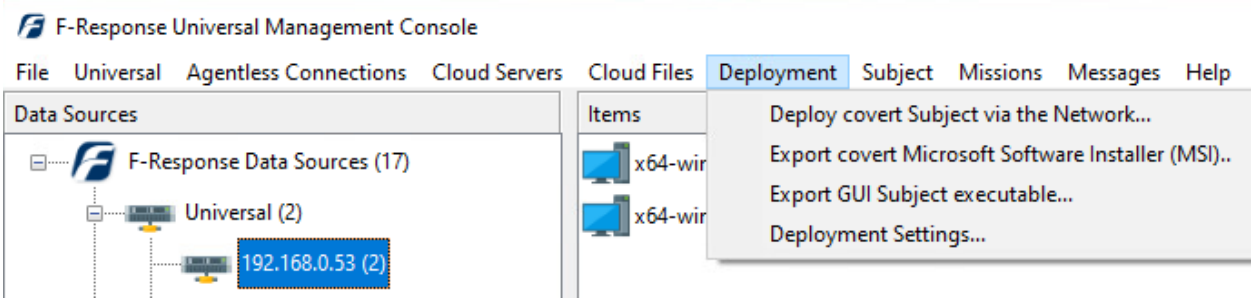
Service Executable: This is the executable name that will be assigned when the subject software is deployed.

Wait Hint: The number of seconds the service will wait before checking into the Universal server. The default is 1 hour (3600 seconds), this is used when the server is in filtered mode or mission mode.

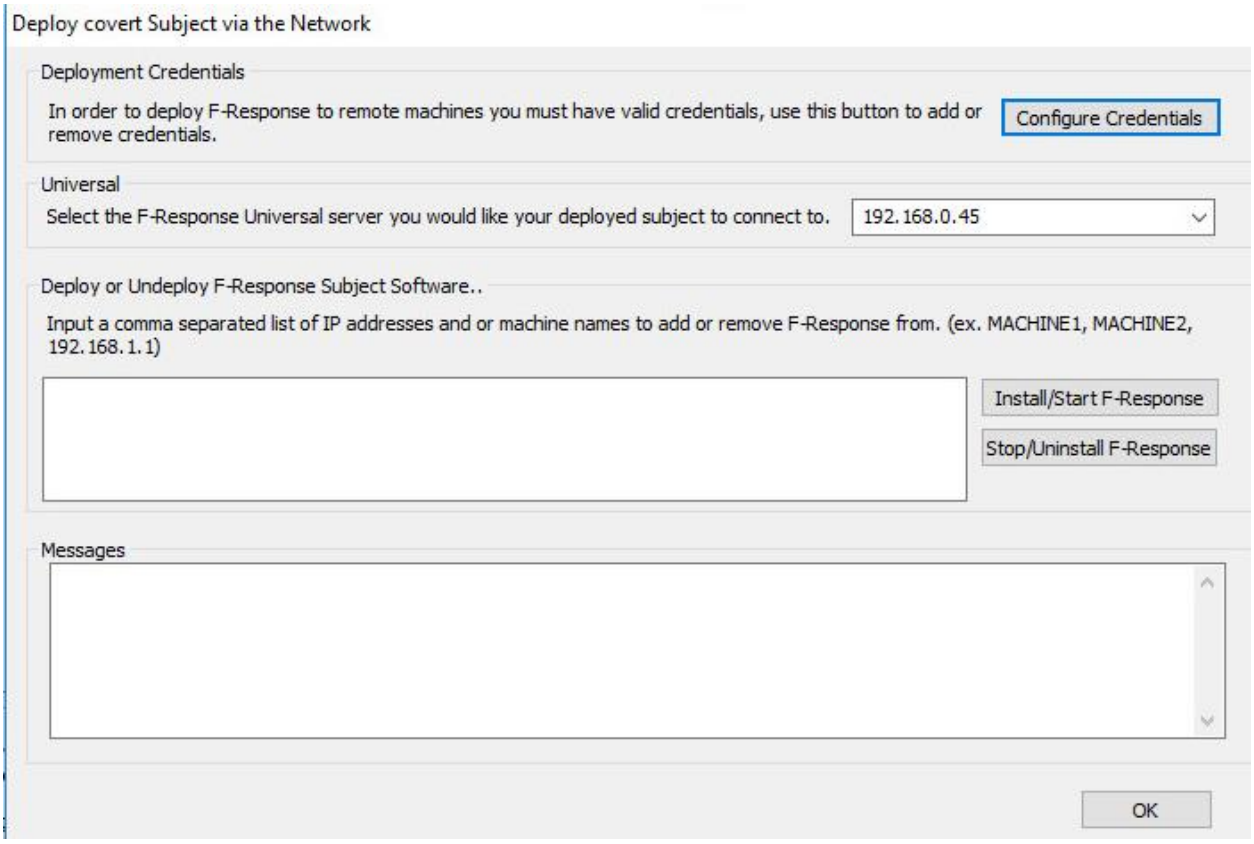
Set Windows Service Startup: If deploying via MSI, the service will be deployed in the "off position", check this box if the service should start when installed.

Deployment using the Management Console

F-Response can be pushed covertly to remote subjects in the environment using the Universal Management Console. **Note: Deployment occurs directly between the examiner and remote subject computer(s) and not through the Universal server.** To deploy F-Response from the console, choose **Deploy covert Subject via the Network…** from the **Deployment** drop down menu.

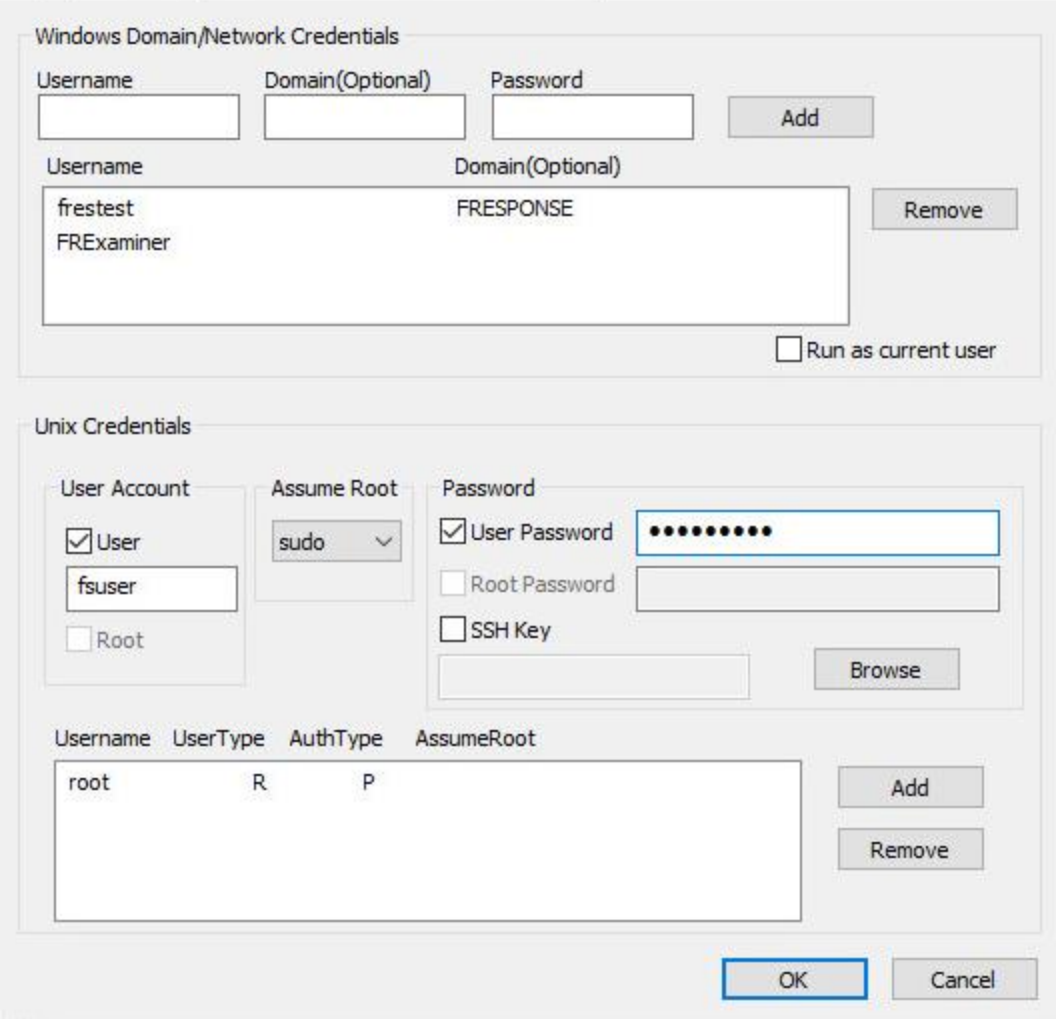


This will open the **Deploy covert Subject via the Network** window. There are 4 sections here: **Deployment Credentials**, the **Universal** Server, **Deploy/Undeploy of F-Response**, and **Messages**.



Firstly, you must add credentials for deployment to the remote subject computer(s) by clicking on the **Configure Credentials** button. Here you can enter an account with administrator level credentials on the remote subject computer (F-Response needs admin level credentials on the remote computer to expose and present the resources on the machine).

Deploy covert Subject via the Network Credentials Configure



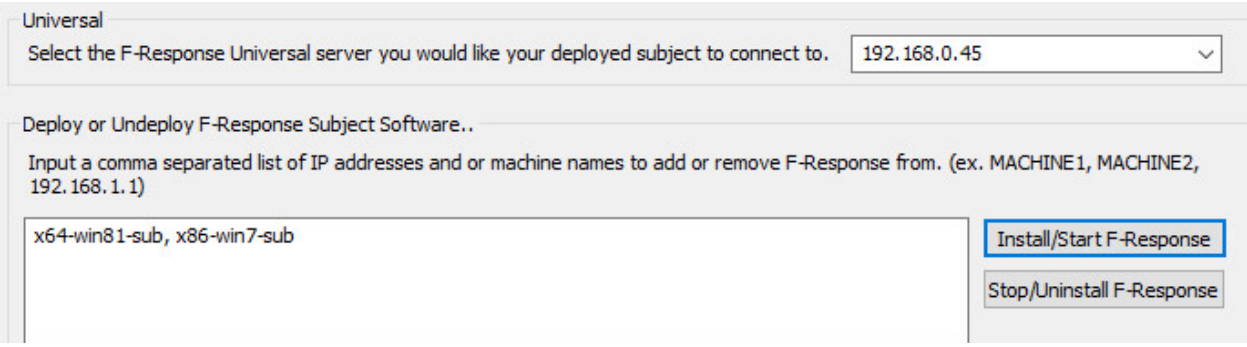
Here credentials can be added for both Windows (top section of the window) and Non-Windows platforms (lower portion of the window).

Under **Windows Domain/Network Credentials**, enter the Username (with administrator level privileges), Domain (if it's a local account leave this field blank), and Password. Click **Add** to add the credential to the stack.

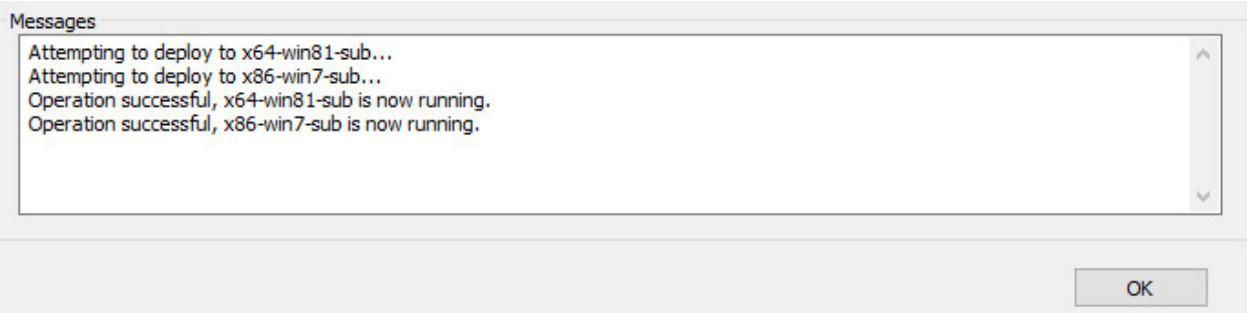
Under **Unix Credentials**, credentials can be added for Apple OSX (be sure SIP is disabled) and Linux subjects. Under **User Account,** check **User** and enter the username. The user account must have elevated privileges to install and run the subject software so select **su** or **sudo** from the drop-down list under **Assume Root**. Next check **User Password** and enter the password for the account. Alternatively, if using the root account, simply select **Root** under **User Account**, check **Root Password** and enter the password. Click Add for each account to add them to the stack.

Click **OK** in the lower right corner once all the credentials have been added to return to the Deployment window.

Next, choose the Universal server the remote subject will use from the drop-down list.



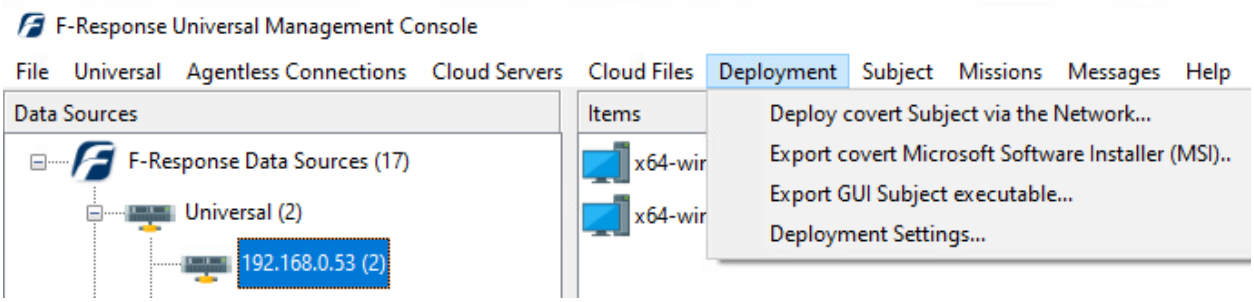
The remote computer(s) can be entered under Deploy or Undeploy by hostname or IP address. Click Install/Start F-Response to scan for and install F-Response on the remote subject(s). Feedback for the results of the search and install can be seen in the messages panel below.



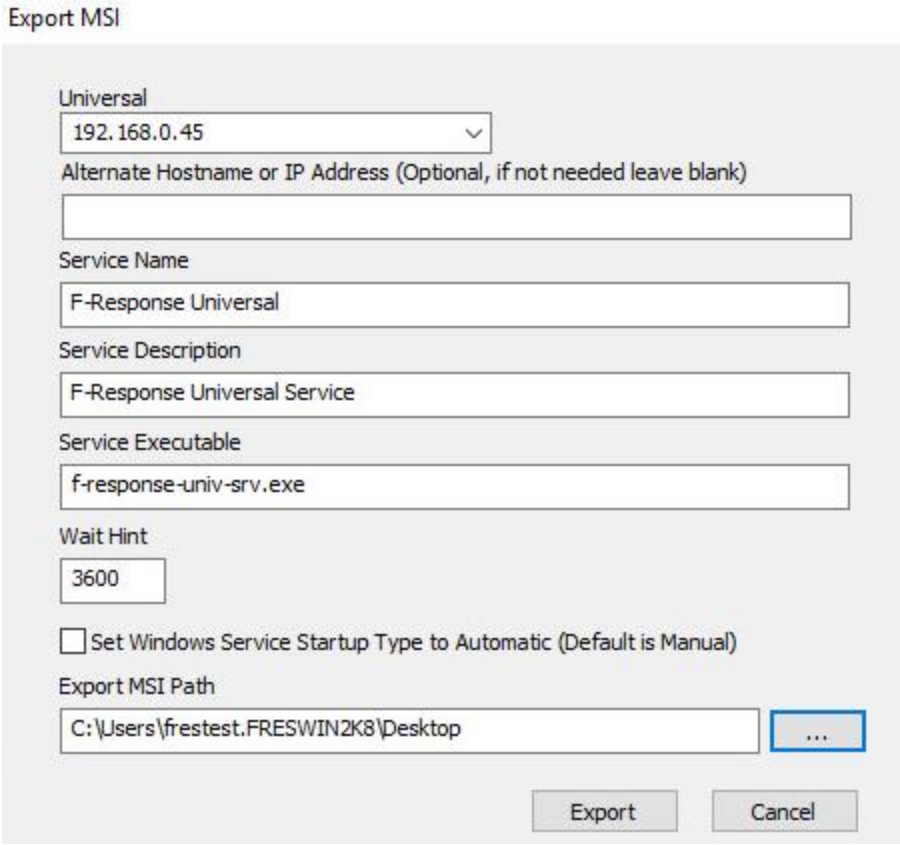
Click OK to return to the console and the remote computers will be listed in the Items column.

Deployment via MSI

F-Response Universal can also be distributed via MSI using a software management system such as SCCM. To create an MSI for distribution, choose **Export covert Microsoft Software Installer (MSI)…** from the **Deployment** drop down menu.



The **Export MSI** window will open, most of these fields will be pre-populated with the information entered under the **Deployment Settings…** option from earlier but they can be modified here before exporting the MSI.



There are 7 fields here to consider:

Universal: Choose the Universal server you would like to use from the drop-down list.

Alternate Hostname or IP Address: (Optional) if a subject cannot reach the Universal server's IP, the external or NAT'd IP can be entered here.

Service Name: Universal runs as a service on the remote subject computer, create a service name that does not conflict with an existing service.

Service Description: Description value that will be assigned to the F-Response subject service when installed on the remote computer(s). This description is completely optional.

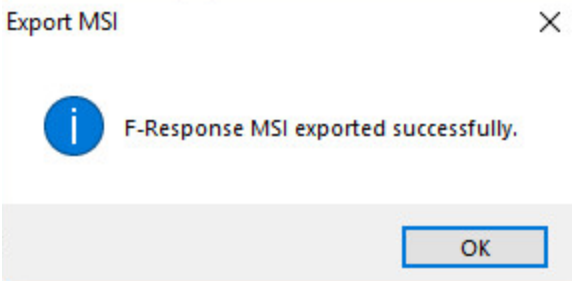
Service Executable: This is the executable name that will be assigned when the subject software is deployed.

Wait Hint: The number of seconds the service will wait before checking into the Universal server. The default is 1 hour (3600 seconds), this is used when the server is in filtered mode or mission mode.

Set Windows Service Startup: The service will be installed in the "off position", check this box if the service should start when installed.

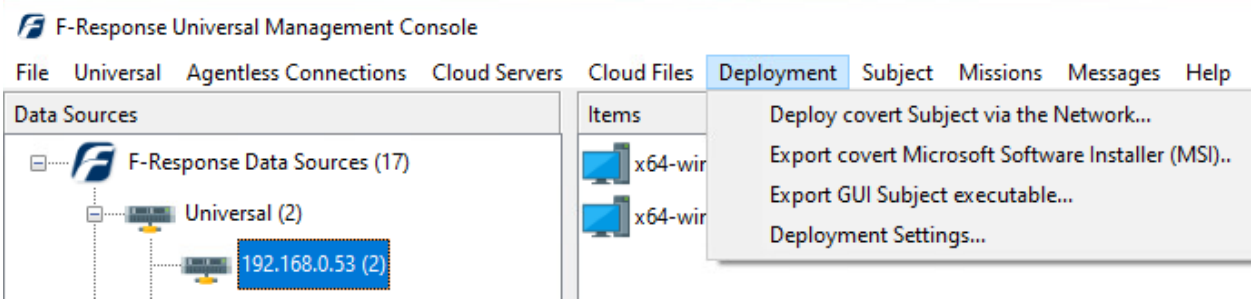
Export MSI Path: The location where you would like to place the MSI.

Click the Export button to create the MSI in the specified folder path and you will receive a notification when the export is complete.

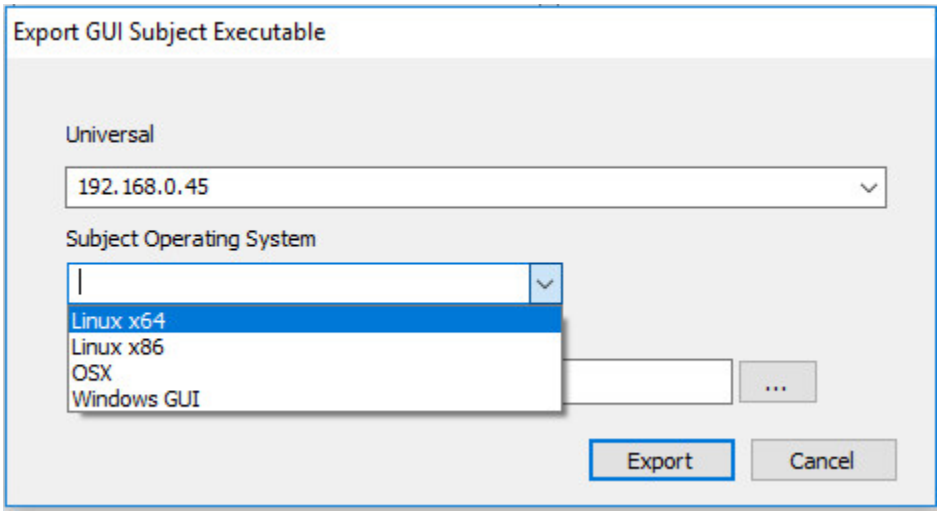


Deployment using an executable

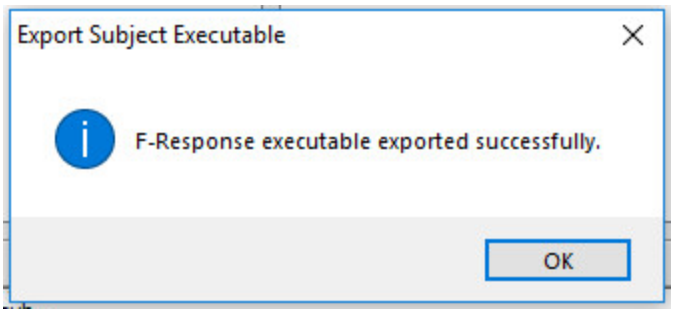
Universal has the option to deploy using an executable file. You can export the appropriate executable file for the remote subject computer from the Management Console under **Deployment** -> **Export GUI Subject executable...**



This will open the **Export GUI Subject Executable** window:



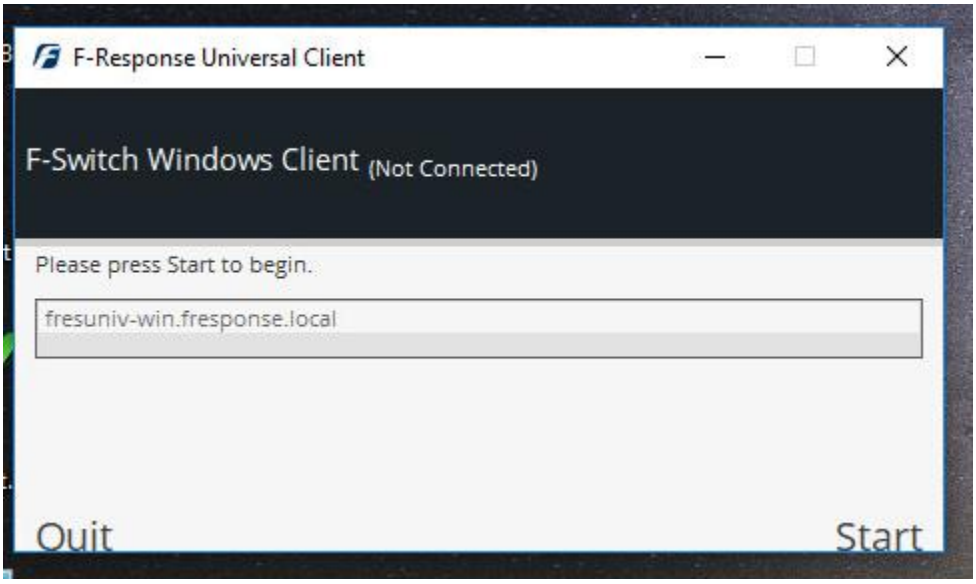
Select the Universal server the subject machine should communicate with from the **Universal** drop-down box. Next, select the operating system running on the remote subject computer from the **Subject Operating System** drop down box. Lastly, enter the location you would like to export the file and click the Export button.



The **Export Subject Executable** window will appear indicating a successful export of the subject executable. This executable can then be copied to and run on the remote subject computer(s).

Windows GUI Subject

Run the executable on the Windows subject computer you wish to investigate. **Note: Do not modify the name of the executable as it contains information needed for the connection.**



Simply click **Start** and the status will change to (Connected), the subject will appear in the Items column in the Universal Console on the examiner computer.

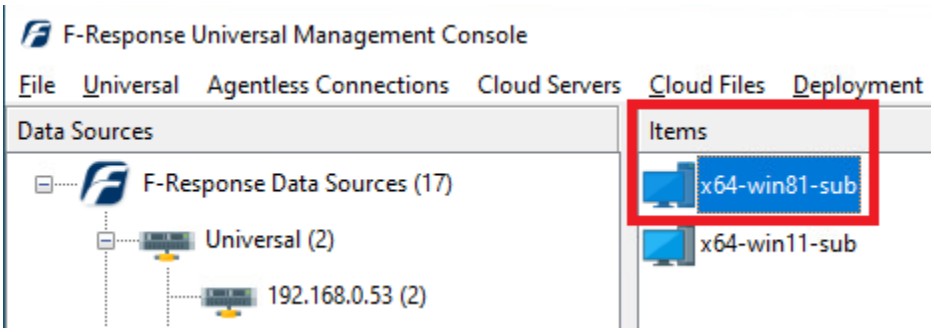
Non-Windows Executables

Export the x64, x86, or OSX executable and copy to the remote computer. Make sure file permissions are set to allow execute and run the executable with root level permissions (su or sudo). The Universal Subject will return a status of Started. Return to the examiner machine and the computer can be seen in the Items column.

```
[root@x64-linux-sub ~]# cd /tmp
[root@x64-linux-sub tmp]# ls
univ-subject-lin64_fresuniv-win.fresponse.local_80_fcfe316a97
[root@x64-linux-sub tmp]#  ./univ-subject-lin64_fresuniv-win.fresponse.local_80_fcfe316a97
F-Response Universal Subject (Linux),(Version 8.0.1.20) Started.
```

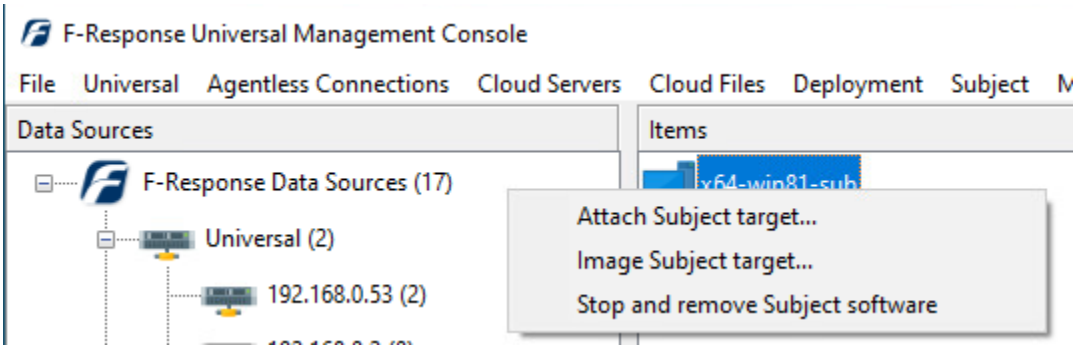
Working with remote subjects

Once F-Response has been successfully installed and is running on the remote subject computer, it will appear in the Universal Management Console in the **Items** column.



Subjects successfully deployed and running will appear under the Universal server they were configured to connect with and can be viewed by selecting the Universal root or the specific Universal server in the leftmost column.

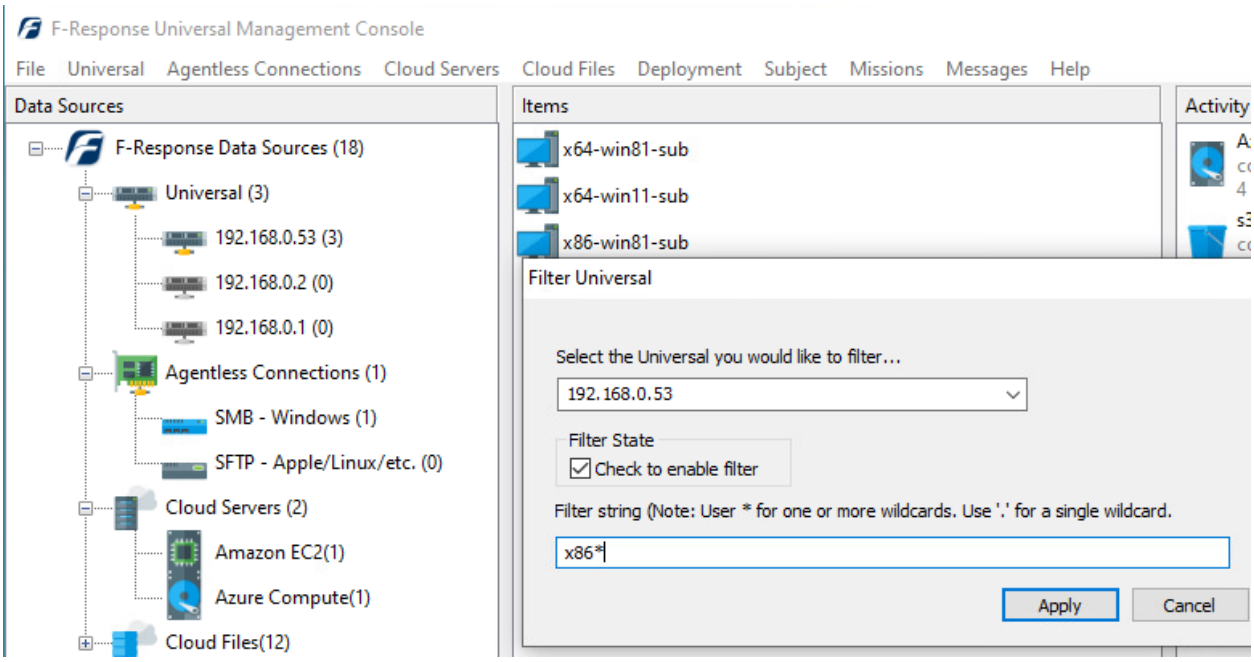
There are 2 choices in interacting with a subject computer: Attaching to a target on the remote machine and adding it as a local drive, or performing a direct image of a drive on the remote machine. These options can be accessed from the Subject drop down menu or by right clicking on the subject in the Items column.



Display Filtering

F-Response highly recommends deploying to subject machines on an as needed basis, but we realize this may not always be feasible. If you are finding the display difficult to navigate, we recommend you use the Display Filtering option to locate a specific subject or subjects of interest.

To activate a Display Filter, choose Universal -> Filter Display… from the menu, or simply right-click on the Universal Server in the Data Sources column and choose Filter Display… .

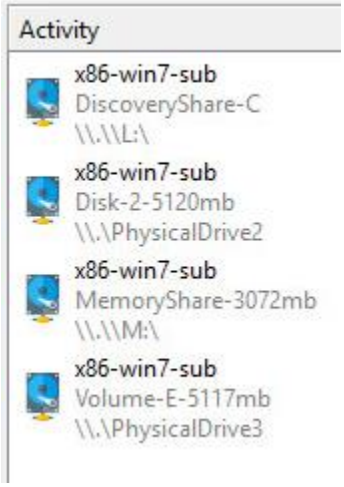


The Filter Universal dialog will open. Choose the Universal server from the dropdown list, then check the box under Filter State to enable the filter. Lastly, enter the string to filter on and click apply. Only subject hostnames that match the filter will then appear in the Items column.

To disable a display filter simply return to the Filter Universal window, choose the Universal Server and clear the Filter State checkbox.

Subject Target types

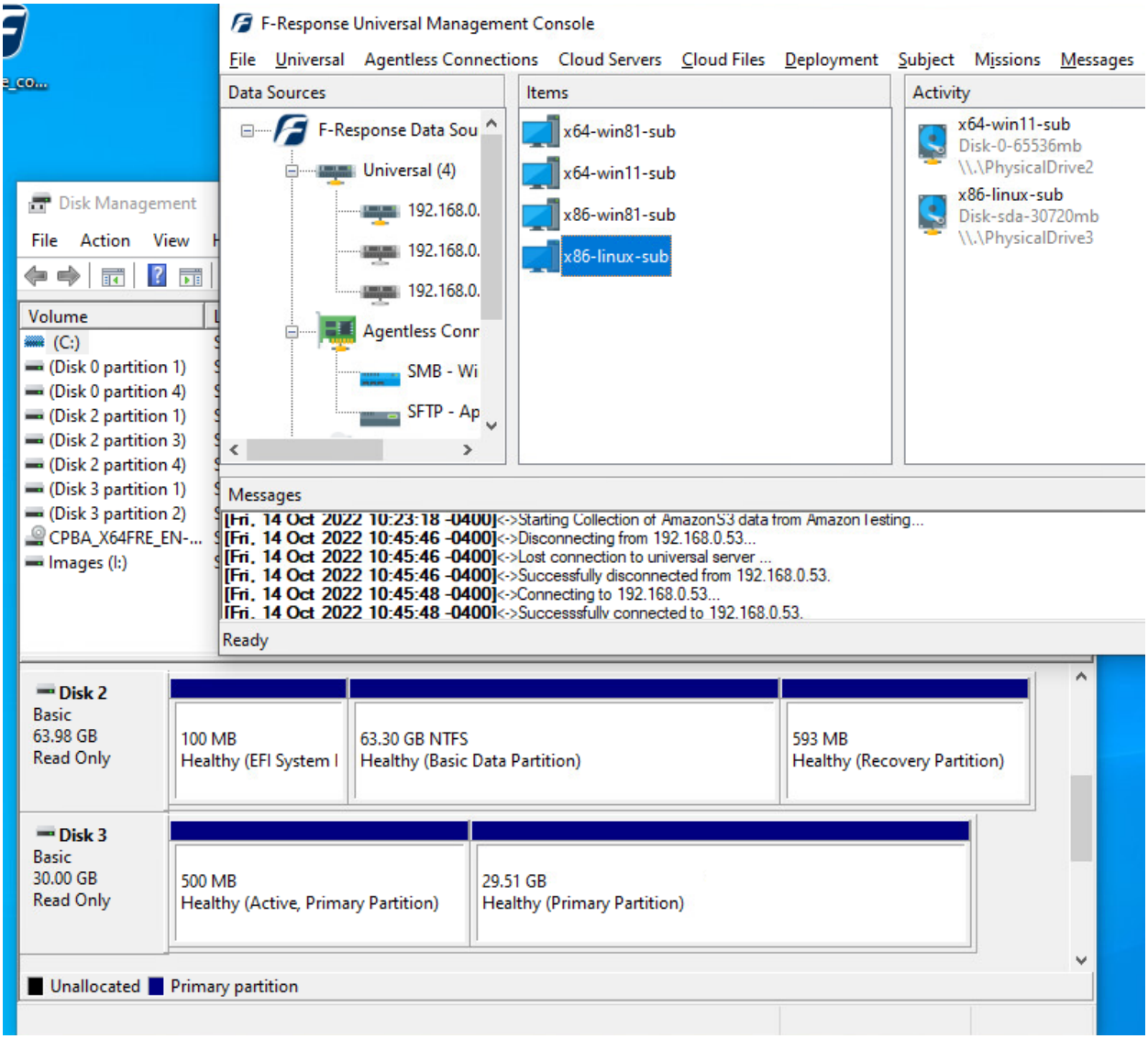
Each remote machine displays different targets based on the operating system. The following list identifies the available Target types, where they are available, and what they represent:



- **Physical Drives, Partitions, and Volumes**
  - F-Response Universal provides a complete SCSI Adapter for presenting remote physical disk(s) as full, read-only local disks.
- **MemoryShares™**
  - **MemoryShares™** provide live physical memory access to remote Windows subject physical memory as a live file, suitable analysis with virtually any incident response product. **Note: This option is only available on Windows subject computers.**
- **DiscoveryShares™**
  - DiscoveryShares™ allow F-Response Universal examiners to access a remote machine's files and folders completely read-only whether they be Windows, Linux, or Apple OSX. DiscoveryShares™ offer a great way for both technical and non-technical users to access a remote machine's files and folders.

Physical Drives, Partitions, and Volumes

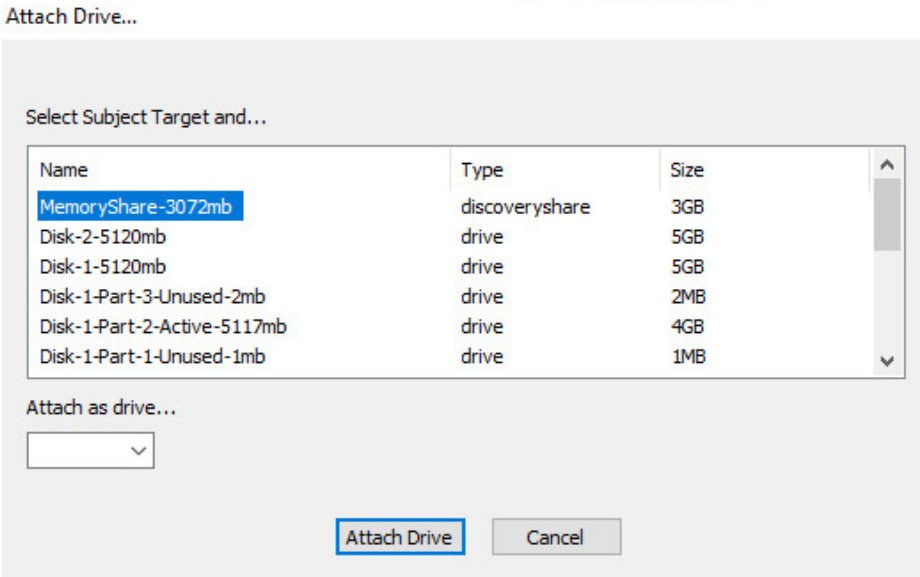
Right click on a computer in the Items column and choose Attach Drive. A list of Targets will be presented which includes physical disks, partitions, and logical volumes. Choose one and click Attach Drive. Once attached access to the full physical device is completely read-only. The attached drive is a full physical device in the context of the examiner machine and will be assigned a physical drive number as seen in Disk Management.



Individual partitions can also be connected separately using the Disk-X-Part-X Targets. Individual partitions will be shown as attached physical drives.

MemoryShares™

A MemoryShare™ on a remote Windows system is added as a share on your examiner computer.



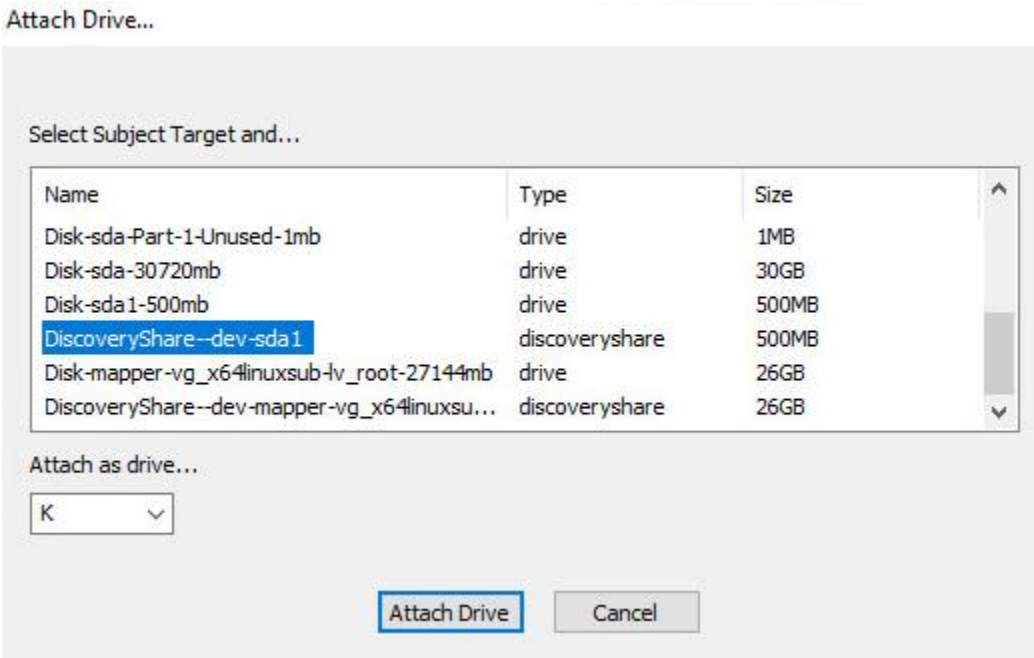
Once attached, access to the complete physical memory of the remote machine is presented via a "live file" on the share.

This live file represents the physical memory of the remote machine in real-time and is not a snapshot or point in time image. Furthermore, this image file can be readily opened and analyzed in applications like Volatility[1] for real time analysis.

[1] http://code.google.com/p/volatility/

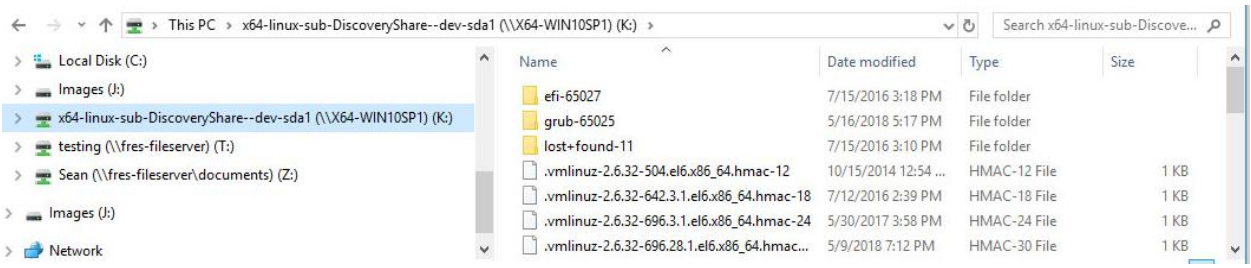
DiscoveryShares™

A DiscoveryShare™ is added as a share on the examiner computer and can be used to access the files and folders on the remote subject.



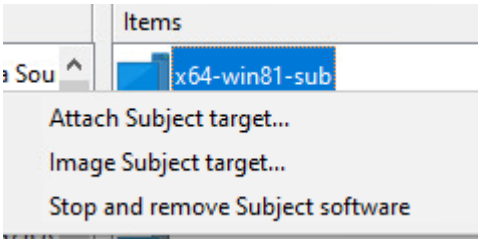
All activity is write-protected by default. **Note: In the case of remote Windows system files, the Windows OS on the examiner computer may elect to apply additional security controls preventing access to certain files.** In such cases, a better approach would be to attach to the drive and leverage a forensic tool to review or collect the data.

Remote Apple OSX or Linux System files and folders can be reviewed with forensic or eDiscovery tools or simply using Windows Explorer natively.

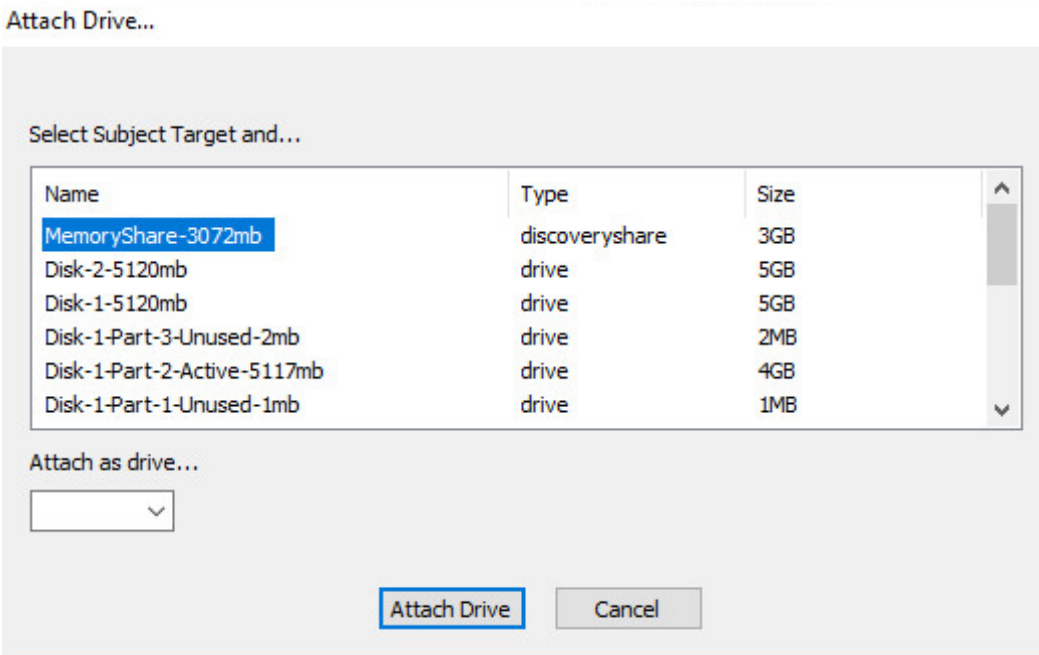


Attaching a Subject Target

Resources on the remote machine can be attached as a write-protected local volume or drive on the examiner computer. Choose **Attach Subject target…** from the menu:

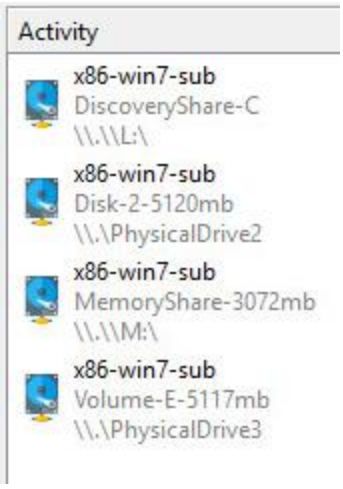


and the **Attach Drive…** window will open:



Choose the target resource on the remote machine and click **Attach Drive** to add as a local disk on the examiner computer. In the case of attaching a **MemoryShare** or **DiscoveryShare**, select an available drive letter before clicking **Attach Drive**.

The attached resource on the remote machine will appear in the **Activity** column.



Imaging

Overview

The F-Response Universal Management Console provides a simple and straightforward mechanism for creating complete images of F-Response devices and targets. This imaging capability is completely optional however, since F-Response devices are vendor neutral you are welcome to use whatever imaging or analysis tools you would like. We recommend leveraging additional imaging tools if you require a targeted file collection or need a specific image format other than the evidence file format (e01).

Imaging methods and recovery

There are two methods to approach imaging from the Console, direct imaging and disk imaging.

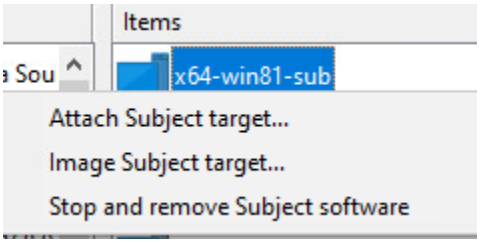
Choose direct imaging (i.e., imaging the subjects targets directly without attaching to the remote resource on the computer) in situations where you have anti-malware tools or AV on your examiner computer that might want to scan the attached disk. Direct Imaging can hand small drops in connectivity between the examiner computer and the Universal server. Image resumption will be automatic once the examiner computer reconnects.

Choose disk imaging (i.e., imaging the subject target disks after attaching to the remote resource on the computer) if you believe the subject is likely to go offline for an extended period of time, or may change network address when it returns. Physical disk imaging does have the ability to resume when the subject computer loses connection, however resumption is manual and requires reattaching the device in question.

Creating a Direct Image from the Console

This option allows you to image a remote disk directly without having to attach it as a drive first. This method can handle potential small disruptions in connectivity to the Universal server and actively recover [2]the imaging process.

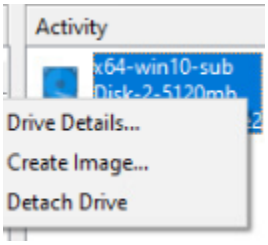
From the Subject drop down menu or by right clicking on the subject in the Items column, select **Image Subject target…**



This will open the **Create Image…** window.

Creating a device physical image from the Console

After successfully attaching one or more remote targets to the local examiner machine, you can right-click on the physical device and select **Create Image…** This will present the imaging dialog where you can select the destination, image name, etc.

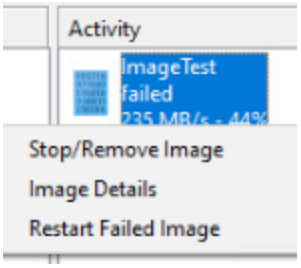


Device Physical Image Resumption

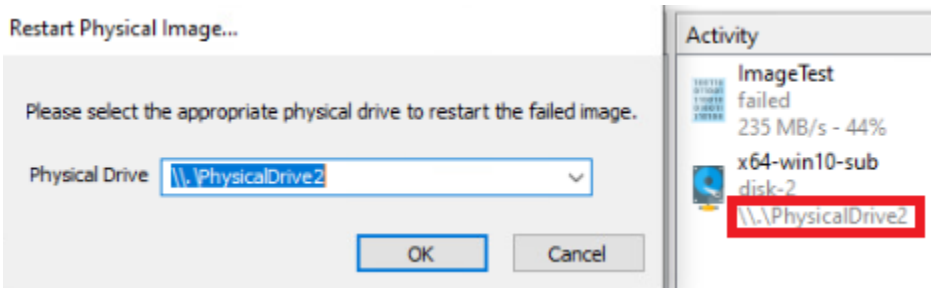
(Does not apply to *Share devices)

In the event of a loss of connectivity (i.e., The target device becomes disconnected and drops from the console) you can reattach to the remote computer and are target, and right-click on the image to "Restart Failed Image".

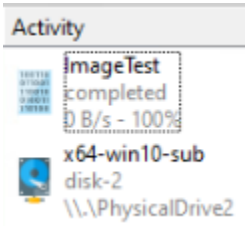
[2] In the event the examiner loses connectivity with the Universal Server. Due to the architecture of the Universal Subject, you will not be able to resume a direct image should it lose connectivity with the Universal Server.



Take note of the physical drive number assigned when reattaching to the remote target. You'll need to select the correct physical drive from the drop down box in the Restart Physical Image… window.



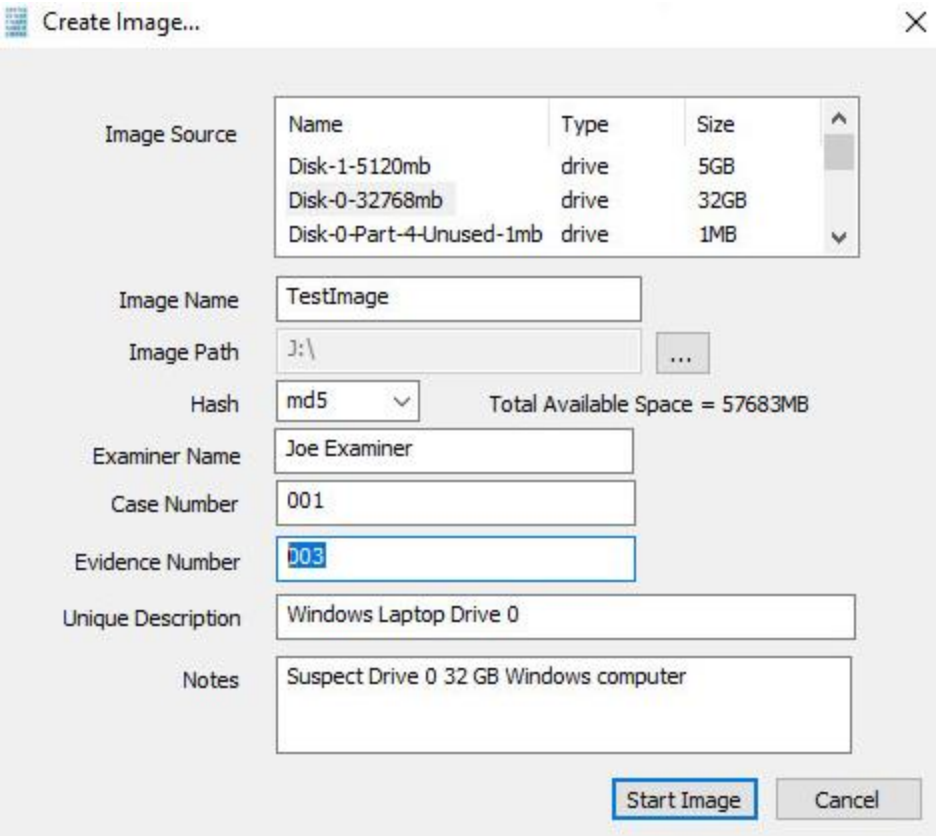
Click OK and the image will continue until complete.



In the event of a loss of connectivity (ie. The target device becomes disconnected) you can now reattach the disk, and right-click on the image to "Restart Failed Image." Restarted images require that you have the source media re-attached and resume "roughly" where they left off.

Creating an Image

After choosing an imaging method and selecting **Create Image…** the window will open with the following details needed for collection:



There are 9 fields here, the first 4 are mandatory and the remaining 5 are optional.

Image Source: If imaging directly, select the disk, partition or volume to image on the remote computer. Note discovery shares and Windows physical memory are not an option to image and therefore not presented.

Image Name: The resulting e01 file name you would like to create

Image Path: The local destination you would like to place the image **Note: Imaging to a network share is not supported.**

Hash: choose md5 or sha1 for the hash value for the image.

Examiner Name: (optional) Assign an examiner name for the collection.

Case Number: (optional) Assign a Case Number for the collection.

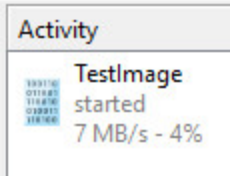
Evidence Number: (optional) Assign an Evidence Number for the collection

Unique Description: (optional) Create a short description for the collection.

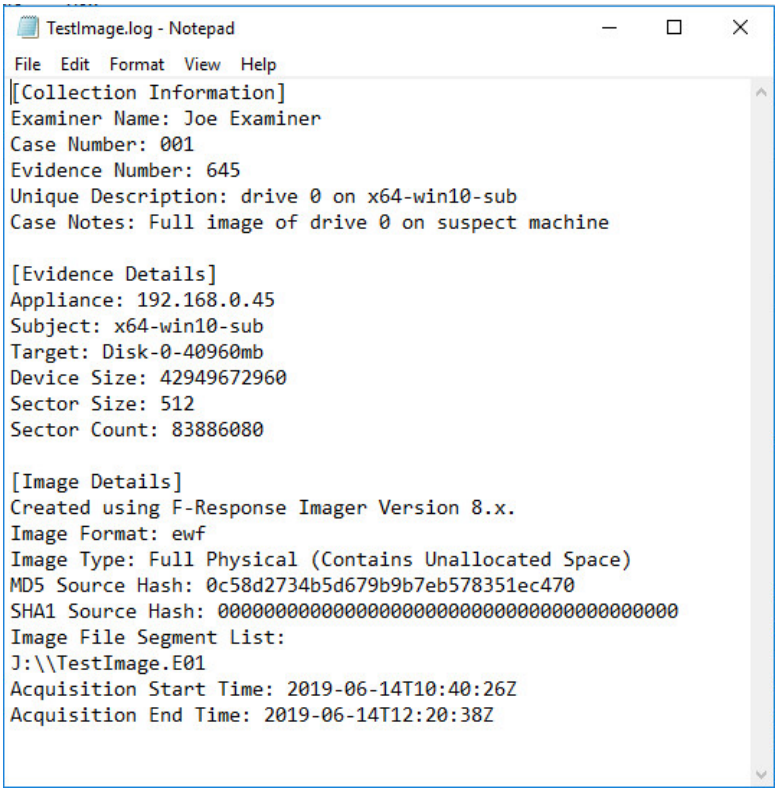
Notes: (optional) Enter any additional notes for the collection.

All the information entered in the optional fields will be added to the final collection log file along with the e01.

Click **Start Image** to begin the imaging process



When completed, the e01 and log file can be found in the destination folder.




```
[Collection Information]
Examiner Name: Joe Examiner
Case Number: 001
Evidence Number: 645
Unique Description: drive 0 on x64-win10-sub
Case Notes: Full image of drive 0 on suspect machine

[Evidence Details]
Appliance: 192.168.0.45
Subject: x64-win10-sub
Target: Disk-0-40960mb
Device Size: 42949672960
Sector Size: 512
Sector Count: 83886080

[Image Details]
Created using F-Response Imager Version 8.x.
Image Format: ewf
Image Type: Full Physical (Contains Unallocated Space)
MD5 Source Hash: 0c58d2734b5d679b9b7eb578351ec470
SHA1 Source Hash: 0000000000000000000000000000000000000000
Image File Segment List:
J:\\TestImage.E01
Acquisition Start Time: 2019-06-14T10:40:26Z
Acquisition End Time: 2019-06-14T12:20:38Z
```

Log File Example

Mission Mode

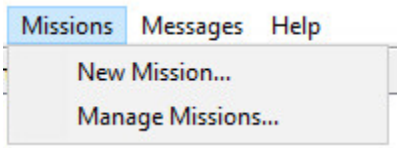
Overview

The mission system can be employed for tighter controls and segregation of duties. Mission mode can be used with an as-needed or pre-deployment model and can be used under local or active directory authentication. Once Mission mode is enabled on the Universal server, examiners must create a mission and add the machines they wish to view in the console to that mission. Remote subject computers running F-Response will not be visible in the console unless added to a mission.

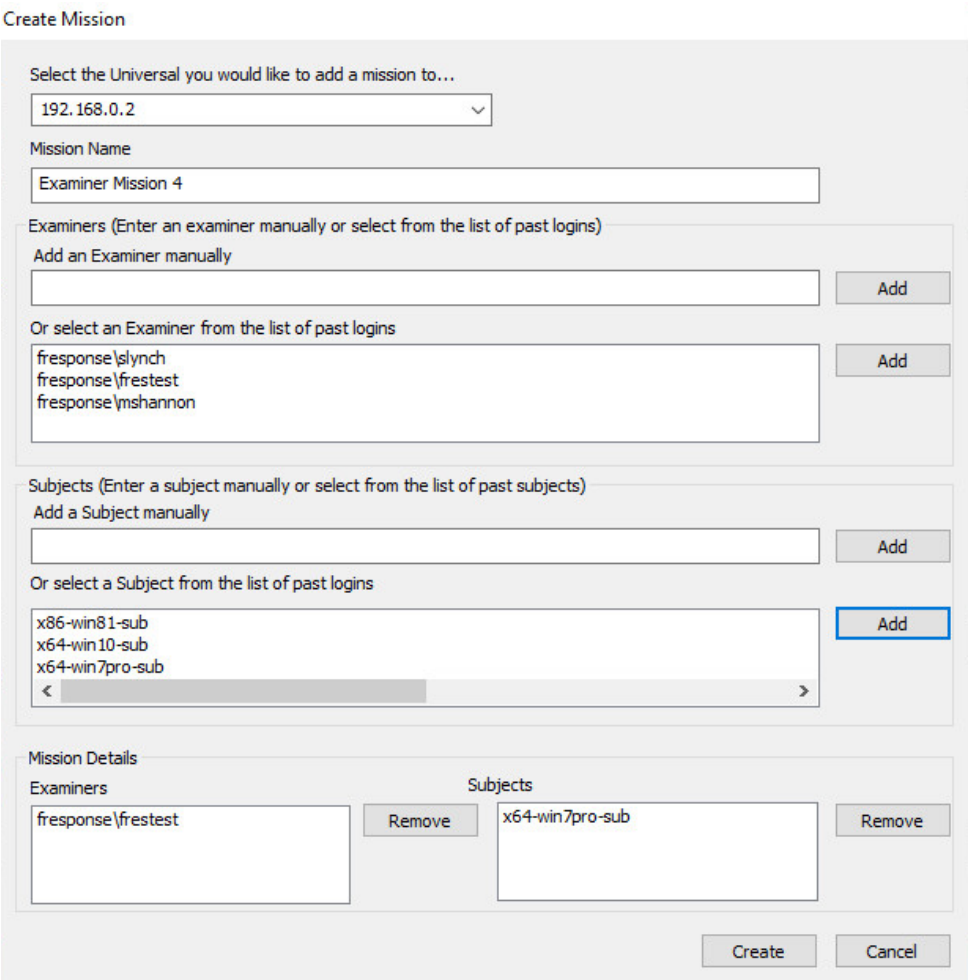
Creating a Mission

Please note that once a mission is created it cannot be altered. A subject computer can only exist in a single mission at any time.

To create a mission, choose **Missions - New Mission…** from the drop down in the Console.



This will open the **Create Mission** window:



There are 4 fields to work with:

Universal Server: You must select the Universal server where you wish to create a mission (and this server must be configured for Mission Mode through the Universal Server configuration) from the drop down list.

Mission Name: Create a name for your mission. This will help to identify your project when managing missions later.

Examiners: Here you can add the list of examiners that should have access to the remote systems in the mission. You can choose to add them manually by typing in the account and clicking Add, or by selecting them from the list of previously seen examiners and choosing Add.

Subjects: Here you can add the remote subject computers you wish to see in the console. Simply type in the hostname and click Add, or choose from the list or previously seen computers (scroll horizontally) highlight and click Add.

Mission Details: You can find the full details of your Mission in this section and can adjust accordingly if needed. When you are satisfied with the information simply click the Create button.

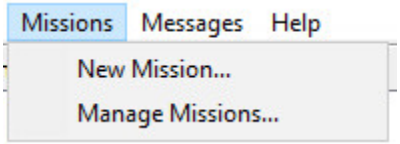
Understanding Missions

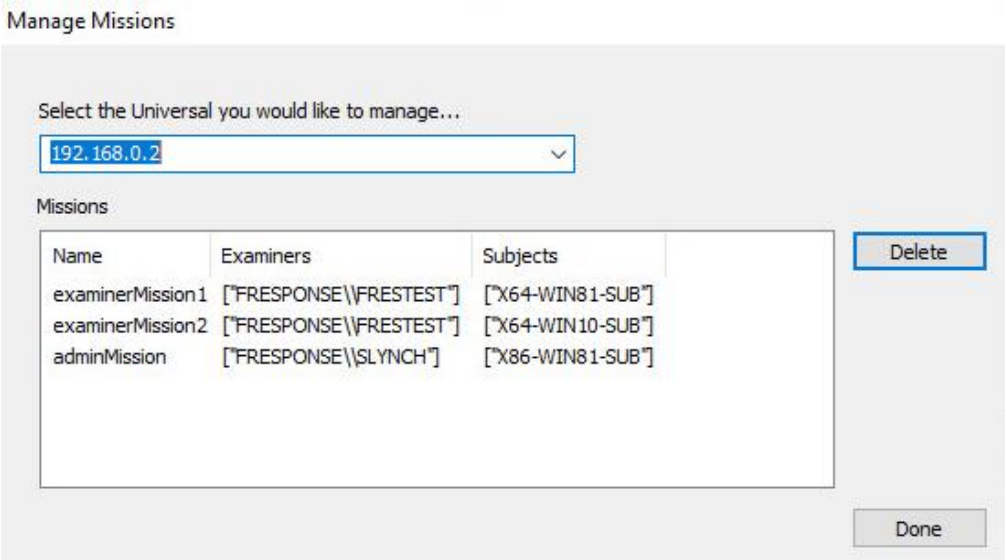
The mission system can be used with an as-needed or pre-deployment model. Regardless of the deployment method used, subject computers running F-Response will "check-in" with the Universal server to see if they are currently assigned to a mission. The period of time it takes for a subject to reach out to the Universal server is determined by the wait hint set in the Deployment Settings. Once the subject computer registers itself as part of a mission it will appear in the console for any examiners who are also part of the mission.

Each mission is specific to the examiner(s) assigned to it. Examiners will not see or have access to subject computers running F-Response unless they are part of a created mission, nor can they see machines tasked to another examiner's mission.

Managing Missions

Examiners can manage only their own missions. Administrators can manage all active missions in the system (*Note, administrators cannot see subjects in the console unless they also have been added to a mission). To manage active missions, choose **Missions -> Manage Missions…** from the drop-down menu in the Console.





From the Manage Missions window select the Universal server from the drop-down menu to view the list of missions. Again, Examiners will only see missions they are a part of listed here; Administrators will see the full list of active missions in the system.

The Manage Missions window will show the mission name, then list the examiners and subject computers assigned to the mission. Use the Manage Missions window to review your active missions and delete any that are no longer needed. Deleting a mission does not remove F-Response from the remote subject computer (deployment is managed separately) but the subjects will no longer be visible in the console.

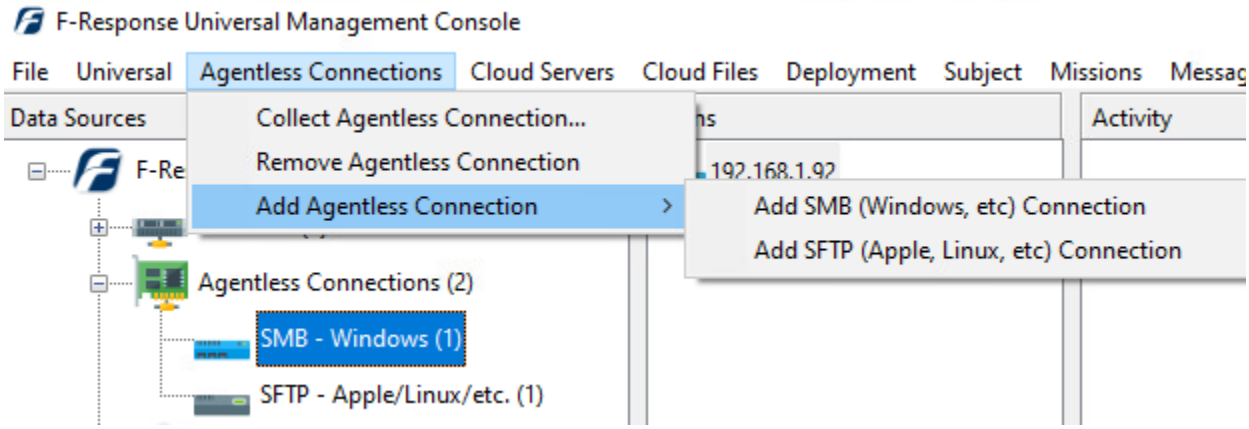
Agentless Connections

F-Response offers agentless collection from remote subject machines leveraging SMB and SFTP connections

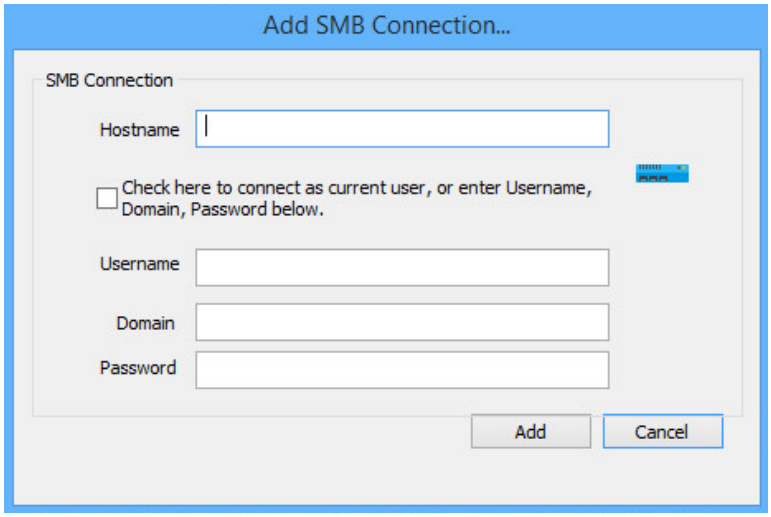
SMB Connection (Windows Systems)

The SMB protocol (present on most Windows systems and NAS[3] devices) is a simple way to collect to a local directory while preserving files dates/times.

To configure an SMB connection, select **Agentless Connections** from the dropdown menu, then **Add Agentless connection →Add SMB (Windows, etc) Connection**, or simply double click **SMB -Windows** in the Data Sources column to bring up the **Add SMB Connection** window.



Add SMB Connection…



Add Agentless SMB Connection dialog…

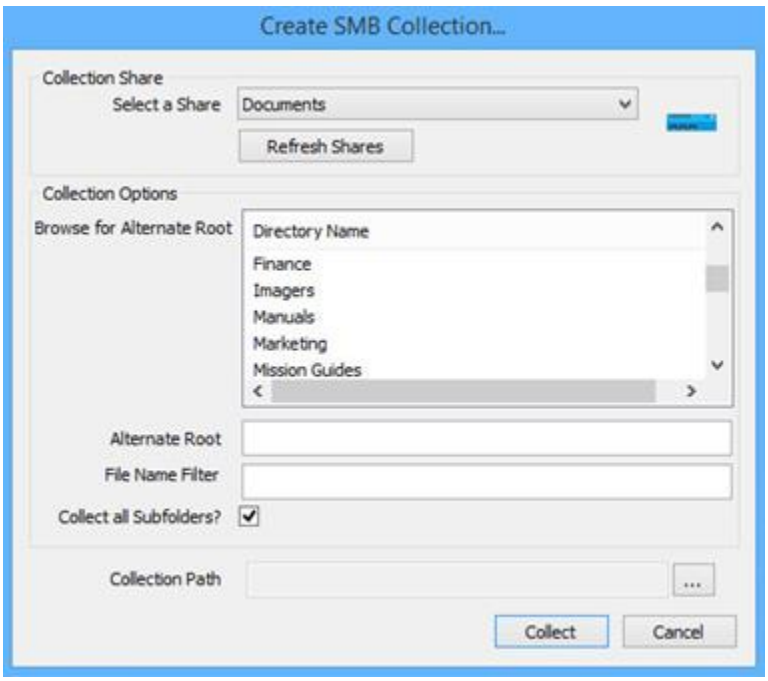
[3] Network Attached Storage.

Use the "Add SMB Connection…" dialog to input a new connection. You will need the hostname or IP of the remote computer and sufficient credentials for access[4]. Click the **Add** button when complete and the hostname will appear in the **Items** column.

You have two credential options. Either using the currently logged in user when attempting to perform the collection, or inputting a username, domain, and password value. If you use the currently logged in user, be sure to note that the software will not save your user information, and will instead execute any collection as the current management console user at the time.

Once the host has been added to the Items column a collection can be created. To open the **Create SMB Collection…** window, highlight the hostname in the **Items** column and choose **Collect Agentless Collection…** from the **Agentless Connections** drop-down menu, or simply double click the hostname in the **Items** column.

First, select the share from the **Select a Share** dropdown box.



Under the **Collection Options** portion of the window, there are a few options available to adjust the scope of a collection. Browse through the **Directory Name** to locate a specific directory if needed. The directory chosen will populate the **Alternate Root** field below. The collection scope can be narrowed further by adding a **File Name** filter[5], such as "**pdf**" to collect only files with pdf in the filename.

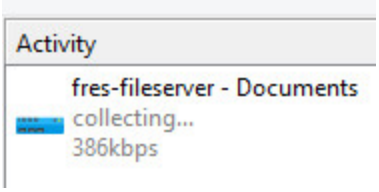
You may choose to tighten the scope further by selecting or deselecting the **Collect all Subfolders?** option. Turning this off will mean only the content of the selected folder is collected, any subfolders will be ignored.

Lastly, choose a location to store the collected data under **Collection Path.**

When ready, click the Collect button to begin the collection. The collection will appear in the Activity column.

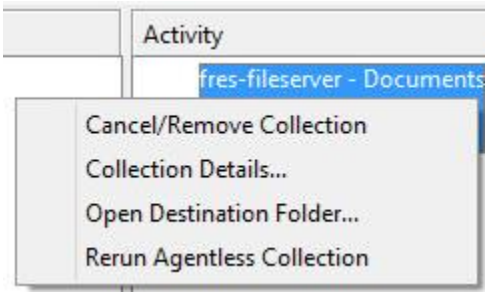
[4] Note: Regardless of credential levels used (Admin, Domain Admin), some system files may be locked by the OS and unavailable for collection using SMB.

[5] The filename filter simply compares the inputted text against the name of the file. For example, by inputting "pdf" both "this_is_not_a_pdf.txt" and "this_is_a_pdf.pdf" would be collected. To limit on file extension, simply add a period to the front. I.e. ".pdf"



Active collection activity…

Completion will be noted in the activity window. You may right click on the collection for a list of options:



Cancel/Remove Collection will cancel a running collection or remove a completed collection from the activity column. This action will not delete the collected data from the storage location.

Collection Details… will provide a quick summary of the collection such as the number of files copied, current collection state, collection duration, etc.

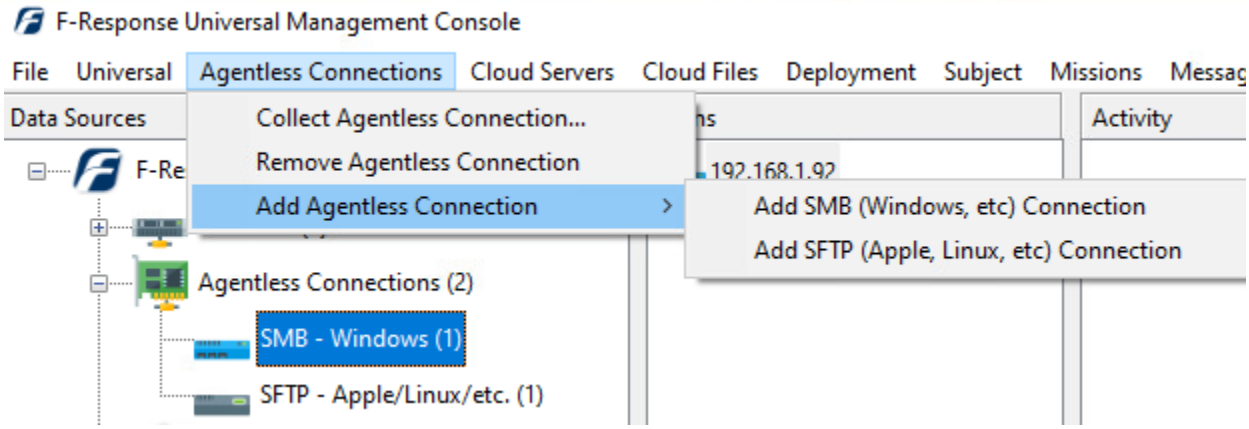
Open Destination Folder… will open the location chosen to store the collection to review the data.

Rerun Agentless Collection If errors occurred for specific files during collection, this option will execute the collection again, focused only on the uncollected files. **This option is only available when collecting to a Local Directory.**

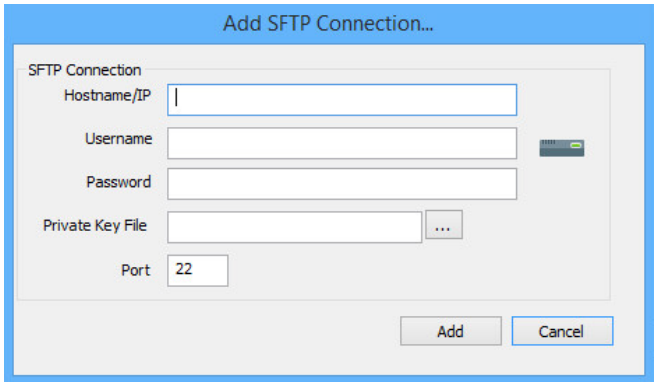
SFTP Connection (Non-Windows)

Secure FTP or SFTP is a common file sharing protocol on Non-Windows operating systems (Apple OSX, Linux, Solaris, AIX, etc.) SFTP can be used to collect to a local directory while preserving file dates/times.

To configure a SFTP connection, select **Agentless Connections** from the dropdown menu, then **Add Agentless connection →Add SFTP (Apple, Linux, etc) Connection**, or simply double click **SFTP - Apple/Linux/etc.** in the Data Sources column to bring up the **Add SFTP Connection** window.



Add SFTP Connection…



Add SFTP Connection Dialog

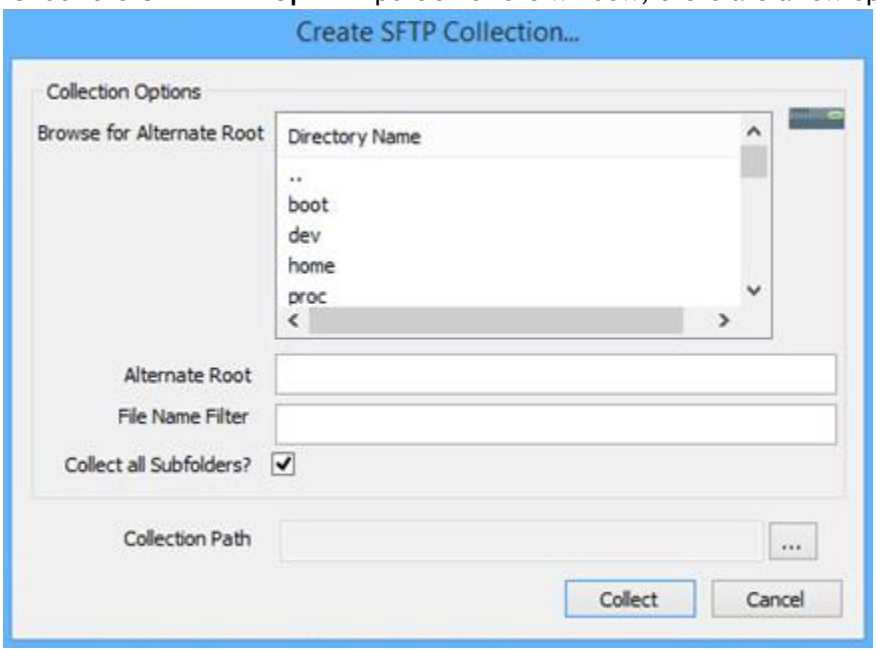
Use the "Add SFTP Connection…" dialog to input a new connection. You will need the hostname or IP of the remote computer and sufficient credentials for access[6]. Click the **Add** button when complete and the hostname will appear in the **Items** column.

If a **Private Key File** is needed it can be added in this field, and the Port can be adjusted if the remote computer is not using the default port, TCP port 22. Click the **Add** button when complete and the hostname or IP will appear in the **Items** column.

[6] Note: Regardless of credential levels used (root), some system files may be locked by the OS and unavailable for collection using SFTP.

Once the host has been added to the Items column a collection can be created. To open the **Create SFTP Collection…** window, highlight the hostname in the **Items** column and choose **Collect Agentless Collection…** from the **Agentless Connections** drop-down menu, or simply double click the hostname in the **Items** column.

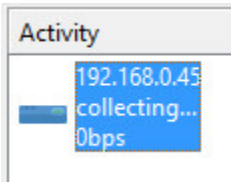
Under the **Collection Options** portion of the window, there are a few options available to adjust the scope of a collection. Browse through the **Directory Name** to locate a specific directory if needed. The directory chosen will populate the **Alternate Root** field below. The collection scope can be narrowed further by adding a **File Name** filter[7], such as **"pdf"** to collect only files with pdf in the filename.



You may choose to tighten the scope further by selecting or deselecting the **Collect all Subfolders?** option. Turning this off will mean only the content of the selected folder is collected, any subfolders will be ignored.

Lastly, choose a location to store the collected data under **Collection Path.**

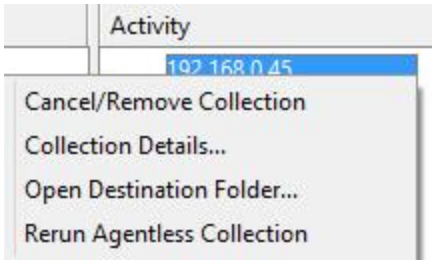
When ready, click the Collect button to begin the collection. The collection will appear in the Activity column.



Active Collection Activity…

[7] The filename filter simply compares the inputted text against the name of the file. For example, by inputting "pdf" both "this_is_not_a_pdf.txt" and "this_is_a_pdf.pdf" would be collected. To limit on file extension, simply add a period to the front. I.e. ".pdf"

Completion will be noted in the activity window. Right click on the collection for a list of options:



Cancel/Remove Collection will cancel a running collection or remove a complete collection from the activity column. This action will not delete the collected data from the storage location.

Collection Details… will provide a quick summary of the collection such as the number of files copied, current collection state, collection duration, etc.

Open Destination Folder… will open the location chosen to store the collection to review the data.

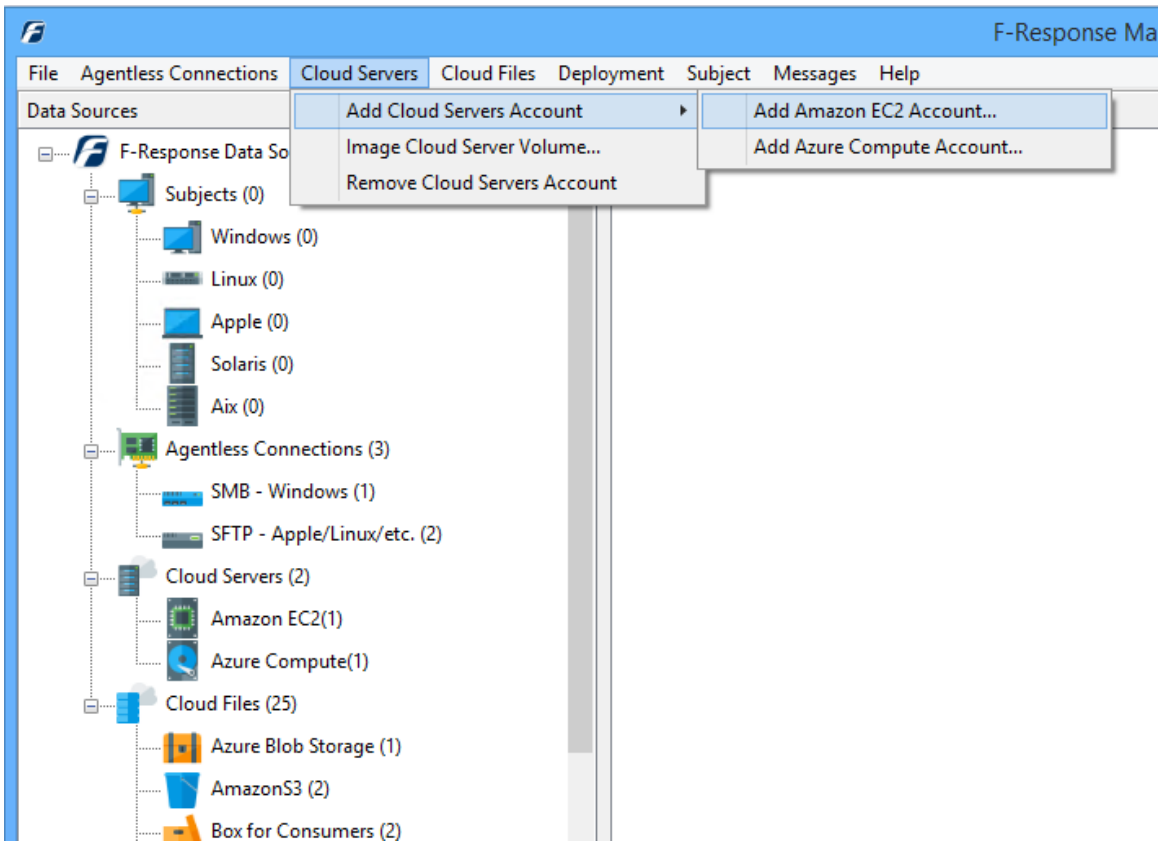
Rerun Agentless Collection If errors occurred for specific files during collection, this option will execute the collection again, focused only on the uncollected files. **This option is only available when collecting to a Local Directory.**

Collecting from Cloud Server Providers

Using the Management Console to collect Cloud Server Volume Snapshots

Disclaimer: F-Response provides access to 3rd party data sources via Application Programming Interfaces (APIs) and internal structures presented by the provider. 3rd party provided data sources are by their very nature volatile. F-Response products provide "best effort" for accessing and interacting with those 3rd party data sources however service disruptions, API changes, provider errors, network errors, as well as other communications issues may result in errors or incomplete data access. F-Response always recommends secondary validation of any 3rd party data collection.

The F-Response Management Console offers the ability to collect cloud server volume snapshots from multiple cloud computing providers. For a complete list of options as well as details on how to leverage this capability, please refer to the provider specific Mission Guide[8] on our website.



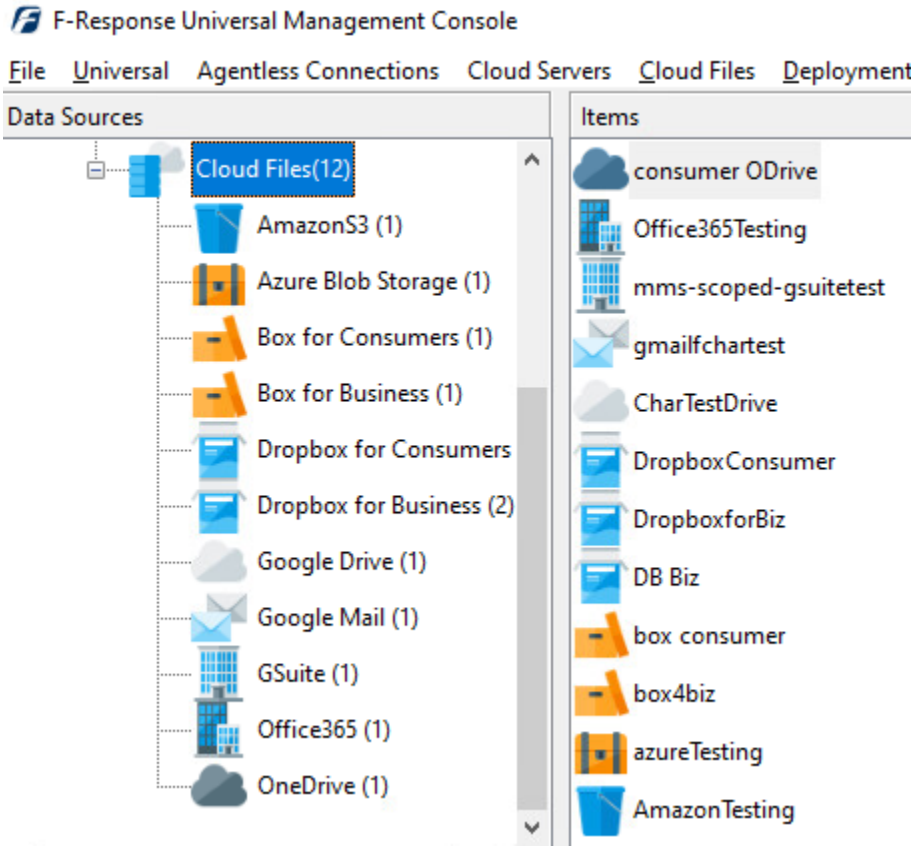
F-Response Cloud Servers Providers

[8] *Mission Guides are specific training documents available for a wide array of topics on the F-Response Website at https://www.f-response.com/support/missionguides*

Collecting from Cloud Files providers

Disclaimer: F-Response provides access to 3rd party data sources via Application Programming Interfaces (APIs) and internal structures presented by the provider. 3rd party provided data sources are by their very nature volatile. F-Response products provide "best effort" for accessing and interacting with those 3rd party data sources however service disruptions, API changes, provider errors, network errors, as well as other communications issues may result in errors or incomplete data access. F-Response always recommends secondary validation of any 3rd party data collection. *For the latest details on collecting from specific cloud providers, please refer to the Mission Guides on our website: https://f-response.com/support/missionguides*

The F-Response Management Console offers the ability to perform cloud provider data collections to native directory locations. All supported providers (which varies by F-Response License) are visible in the Data Sources pane. Configuring access to these providers varies greatly by provider, therefore for the most accurate information see the appropriate Mission Guide[9] on the F-Response Website.

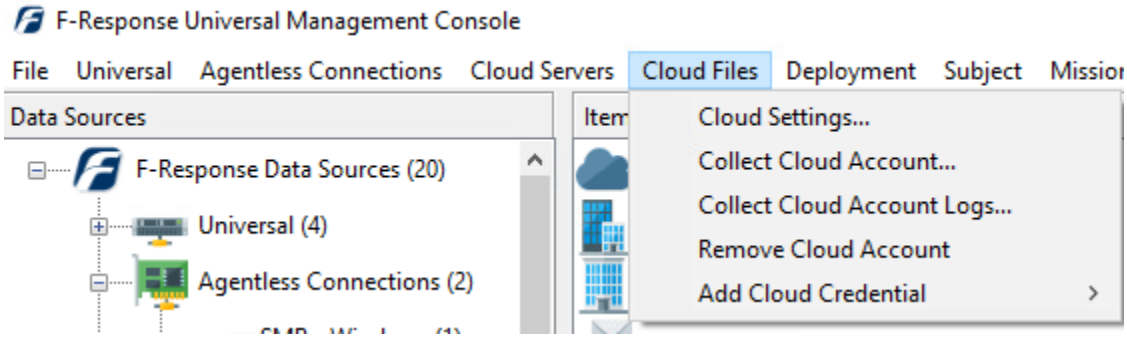


F-Response Cloud Providers

9 Mission Guides are specific training documents available for a wide array of topics on the F-Response Website at https://www.f-response.com/support/missionguides

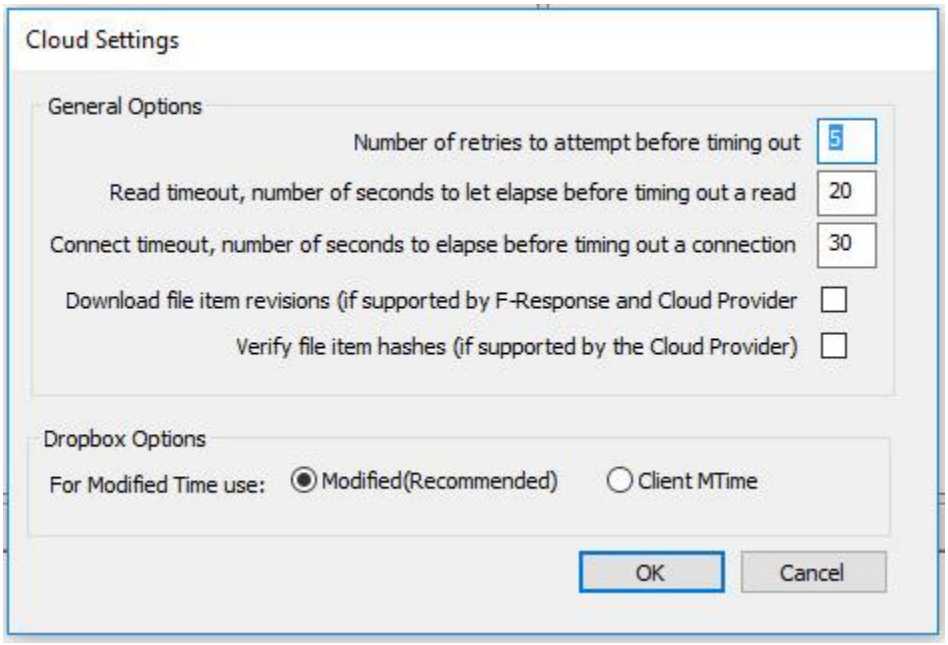
Configuring Cloud Settings

The **Cloud menu** gives us the ability to access **Cloud Settings** and **Credentials**. Using the **Cloud Settings** we can configure both provider specific and application wide settings for communicating with cloud and 3rd party data providers.



Cloud Menu

There are many options that can be configured for communicating with Cloud Providers, these options include:



Cloud Provider Settings

NUMBER OF RETRIES TO ATTEMPT BEFORE TIMING OUT

Setting this number instructs the software to attempt this many web operations before giving up on the request.

READ TIMEOUT, NUMBER OF SECONDS TO ELASPE BEFORE TIMING OUT A READ

Setting this number instructs the software to wait this many seconds before timing out a read attempt.

CONNECT TIMEOUT, NUMBER OF SECONDS TO ELAPSE BEFORE TIMING OUT A CONNECTION

Setting this number instructs the software to wait this many seconds before timing out a connection attempt.

DOWNLOAD FILE ITEM REVISIONS (IF SUPPORTED BY F-RESPONSE AND CLOUD PROVIDER)

Some cloud providers store multiple revisions of a given item. If this option is enabled and both F-Response and the provider support revisions, multiple file revisions (where accessible) will be downloaded.

VERIFY FILE ITEM HASHES (IF SUPPORTED BY THE CLOUD PROVIDER)

If this option is enabled and the cloud provider provides file item hashes, F-Response will verify the file items against the hashes immediately after downloading them.

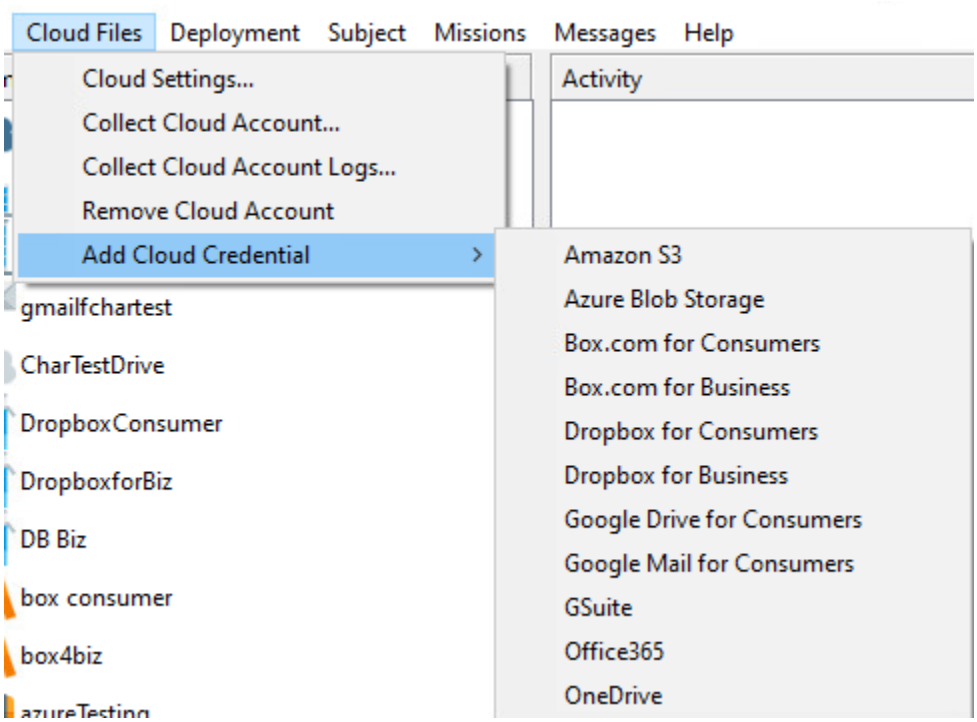
Dropbox Options

FOR MODIFIED TIME USE:

Dropbox provides two different times that can be used as Modified Time for a given file. By default, the software uses the Modified time as provided by the Dropbox Servers. Alternatively, it is possible to use the Client MTime, a non- verified time that is assigned to the files when they are modified by a Dropbox Client tool. The Client MTime is not verified by Dropbox.

Configuring Cloud Credentials

Before you can connect to Cloud services you must first input valid credentials. While the credentials necessary vary by Cloud Provider, all credentials must be input using one of the **Configure Credentials** dialog boxes.

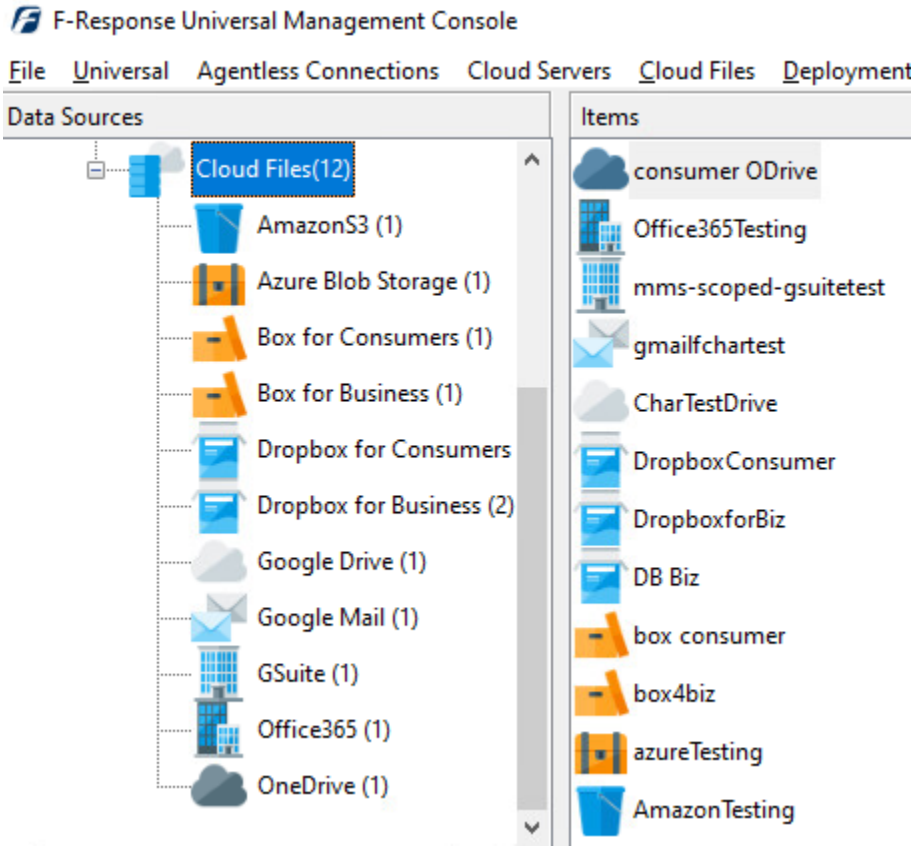


Provider Credentials

As the credential location and process for acquiring those credentials changes frequently for almost all providers, including each one in this manual would quickly become obsolete. Please refer to the specific Mission Guide on the F-Response Website for details on provider you are attempting to access. F-Response Mission Guides are available at https://www.f-response.com/support/missionguides

Collecting a Cloud Account

After successfully adding one or more cloud accounts you will find them visible in the Items column.



Individual and business accounts

Double clicking on an individual account will trigger a dialog for collection of that account, more details on specific dialogs by provider are available in the individual provider Mission Guides on our website: https://f-response.com/support/missionguides

Getting started with the F-Response Management Console (Linux)

Installation

Download and install the **F-Response-Universal-Examiner-Installer-<versionnumber>.rpm/deb** for Linux installation from the F-Response Website: https://f-response.com/support/downloads

Note: You will need your license number to download the software. (Ex: 1777x)

Linux Distribution Compatibility

The Linux examiner is available in Debian and RPM x86_64 packages and has been tested on Centos 6/7, Debian 8, Ubuntu Desktop 14/16, and SIFT3.

Installing Packages

Please refer to your distribution or operating system documentation for more details on appropriately installing packages. For your convenience, the following basic instructions should work for most general Linux and OSX systems.

RPM Installation (Redhat, Centos)

To install the RPM package:

```
# yum install fresponse2univ.x86_64.rpm
```

To uninstall the RPM package:

```
# yum remove fresponse2univ
```

Debian Installation (Debian, Ubuntu)

To install the DEB package:

```
$ sudo dpkg -i fresponse2univ.x86_64.deb
$ sudo apt-get install -f
```

To uninstall the DEB package:

```
$ sudo apt-get remove fresponse2univ
```

Linux Examiner Interface

The examiner and universal interface can be invoked on command line via **fs_exa** or **fs_univ,** respectively. If not, then the environment variable PATH must be updated to include the directory containing fs_exa and fs_univ.

Updating PATH on Linux Bash shell:

```
# export PATH=$PATH:/usr/bin
```

Examiner Interface

The examiner interface is used for the following:

1. Adding and removing appliance entries
2. Starting and stopping appliance clients
3. Querying status of appliance client
4. Changing password of local accounts

An **appliance entry** is an obfuscated configuration file containing the credentials of the user account and the address of the appliance.

An **appliance client** is a process that maintains an active connection to the appliance and provides facilities for the universal interface (see below), such as querying for a list of subjects, stopping a subject agent, and mounting a subject's target.

Universal Interface

The universal interface is used for the following:

1. printing the list of missions, subjects, and targets
2. stopping remote subject
3. mounting and unmounting targets

A **subject** is a host running the F-Response client to expose targets.

A **target** is a disk, volume, or memory on the subject.

Usage Pattern

```
Add the appliance entry      # fs_exa add -u frestest -p frestest -l 192.168.1.83

Start the appliance client   # fs_exa start -l 192.168.1.83 –daemon

List the available targets   # fs_univ list

Mount the target             # fs_univ mount -l 192.168.1.83 -s win10-x64-dev -t DiscoveryShare-C -m . -
                             d
Unmount the target           # fs_univ umount -l 192.168.1.83 -s win10-x64-dev -t DiscoveryShare-C

Stop the appliance client    # fs_exa stop -l 192.168.1.83
```

F-Response Examiner Interface

The examiner interface implements 7 commands:

1. **add** – add appliance entry
2. **remove** – remove appliance entry
3. **status** – print appliance status in csv or json format
4. **start** – start appliance client in foreground or background
5. **stop** – stop appliance client
6. **restart** – performs stop and start command in sequence
7. **pwd** – change local account password

add

The add command creates an obfuscated appliance entry, which contains the user's credentials and appliance address and is stored in /var/lib/f-response/universal/appliance. If the password is not specified on the command line, then the controlling terminal will be prompted to enter the password.

```
# fs_exa add -u frestest -p frestest -l 192.168.1.83
  F-Response Universal Linux Examiner 2.0.1.15
  Copyright F-Response, All Rights Reserved
  Appliance 192.168.1.83 has been added.
```

The default port is 80 (HTTP). The port can be changed by appending a colon and the port number to the -l or –url option.

```
# fs_exa add -u frestest -p frestest -l 192.168.1.83:8080
  F-Response Universal Linux Examiner 2.0.1.15
  Copyright F-Response, All Rights Reserved
  Appliance 192.168.1.83 has been added.
```

remove

The remove command removes an existing appliance entry. Also, any target mounted through the appliance will be unmounted and the appliance client will be stopped prior to the removal of the appliance entry.

```
# fs_exa remove -l 192.168.1.83
  F-Response Universal Linux Examiner 2.0.1.15
  Copyright F-Response, All Rights Reserved
  Successfully unmounted /root/Desktop/win10-x64-dev/DiscoveryShare-C.
  Sent sigterm to appliance 192.168.1.83 process -- 3123
  Waiting for appliance 192.168.1.83 to disconnect ..  success
  Appliance 192.168.1.83 has been removed.
```

status

The status command prints the status of one or more appliance(s) in either CSV or JSON format.

```
# fs_exa status
  appliance,status,system_mode,auth_type,expire_date,subject_count,mission_count
  192.168.1.83,connected,standard,local,12-30-2017,1,0
```

```
# fs_exa status –json
  {
      "appliances": [
          {
              "appliance": "192.168.1.83",
              "auth_type": "local",
              "expire_date": "12-30-2017",
              "mission_count": 0,
              "status": "connected",
              "subject_count": 1,
              "system_mode": "standard"
          }
      ]
  }
```

start

The start command starts an appliance client in the foreground or background depending on whether the -d or –daemon option is specified. If appliance is not specified with the -l or –url option, then all appliances with an appliance entry in /var/lib/f-response/universal/appliance will be started in the background.

```
# fs_exa start -l 192.168.1.83 -d
  F-Response Universal Linux Examiner 2.0.1.15
  Copyright F-Response, All Rights Reserved
  Appliance 192.168.1.83 is on standard mode, uses local authentication, and expires on 12-30-2017.
  Appliance 192.168.1.83 is connected and running in the background.
  Exclude -d,--daemon on command line to run in foreground.
```

```
# fs_exa start
  F-Response Universal Linux Examiner 2.0.1.15
  Copyright F-Response, All Rights Reserved
  Appliance 192.168.1.83 daemon process started (0).
```

stop

The stop command stops an appliance client. If appliance is not specified with the -l or –url option, then all appliances with an appliance entry in /var/lib/f-response/universal/appliance will be stopped. Also, any target mounted through the appliance will be unmounted.

```
# fs_exa stop
  F-Response Universal Linux Examiner 2.0.1.15
  Copyright F-Response, All Rights Reserved
```

```
  Sent sigterm to appliance 192.168.1.83 process -- 3194
  Waiting for appliance 192.168.1.83 to disconnect ..  success
```

restart

The restart command runs the stop and start command in sequence.

```
# fs_exa restart -l 192.168.1.83 -d
  F-Response Universal Linux Examiner 2.0.1.15
  Copyright F-Response, All Rights Reserved
  Sent sigterm to appliance 192.168.1.83 process -- 3249
  Waiting for appliance 192.168.1.83 to disconnect ..  success
  Appliance 192.168.1.83 is on standard mode, uses local authentication, and expires on 12-30-2017.
  Appliance 192.168.1.83 is connected and running in the background.
  Exclude -d,--daemon on command line to run in foreground.
```

pwd

The pwd command changes a local account's password. After the local account password is updated, the appliance client is stopped and the appliance entry is recreated.

```
# fs_exa -l 192.168.1.83 -p frestest pwd
  F-Response Universal Linux Examiner 2.0.1.15
  Copyright F-Response, All Rights Reserved
  Sent sigterm to appliance 192.168.1.83 process -- 3274
  Waiting for appliance 192.168.1.83 to disconnect ..  success
  Appliance 192.168.1.83 has been removed.
  Appliance 192.168.1.83 has been added.
  Updated password for user frestest on 192.168.1.83.
```

F-Response Universal Interface

The universal interface implements 5 commands:

1. **list** – print missions, subjects, and targets
2. **stop** – stop remote subject
3. **mount** – mount target
4. **umount** – unmount target
5. **active** – print mounted targets

list

The list command prints missions, subjects, and targets in either CSV or JSON format.

```
# fs_univ list
  appliance_name,subject_name,target_name,target_type,target_size,block_size,block_count
  192.168.1.83,jching-x64-dev-,DiscoveryShare-C,share,119GB,4096,31431167
  192.168.1.83,jching-x64-dev-,Volume-C-122778mb,raw,119GB,512,251449344
  192.168.1.83,jching-x64-dev-,Disk-0-Part-1-Unused-1mb,raw,1MB,512,2048
  192.168.1.83,jching-x64-dev-,Disk-0-Part-2-Active-100mb,raw,100MB,512,204800
  192.168.1.83,jching-x64-dev-,Disk-0-Part-3-Active-122778mb,raw,119GB,512,251449344
  192.168.1.83,jching-x64-dev-,Disk-0-Part-4-Unused-1mb,raw,1MB,512,2048
  192.168.1.83,jching-x64-dev-,Disk-0-122880mb,raw,120GB,512,251658240
  192.168.1.83,jching-x64-dev-,MemoryShare-5120mb,share,5GB,4096,1310720
```

```
# fs_univ list –json
  {
      "appliances": [
          {
              "name": "192.168.1.83",
```

```
            "subjects": [
                {
                    "id": "7495793870787287257",
                    "name": "jching-x64-dev-",
                    "targets": [
                        {
                            "block_count": "31431167",
                            "block_size": "4096",
                            "case_sensitive": "0",
                            "name": "DiscoveryShare-C",
                            "root_node": "5",
                            "type": "2",
                            "uuid": "1"
                        },
                        …
                    ]
                }
            ],
            "system_mode": 0
        }
    ]
}
```


stop

The stop command stops a remote subject and any target mounted through the subject will be unmounted.

```
# fs_univ stop -l 192.168.1.83 -s win10-x64-dev
  F-Response Universal Linux Examiner 2.0.1.15
  Copyright F-Response, All Rights Reserved
  Checking appliance '192.168.1.83' connection status ... success
  Locating subject ‘win10-x64-dev' on appliance '192.168.1.83' ... success
  Successfully unmounted /root/Desktop/win10-x64-dev/DiscoveryShare-C.
  Unmounting targets from subject 'win10-x64-dev' ... success
  Terminated win10-x64-dev on 192.168.1.83.
```

mount

The mount command mounts a target, such as a disk, volume, and memory, on the specified mount path via the -m or –mount_path option and in either foreground or background mode depending on the -d or –daemon option. There are two types of targets; a raw target represents a disk or volume as a single file while share target represents volume as a set of files and directories. A raw target file can be mounted on loopback on Linux using *mount* for a device file (/dev/loopX) and mounted as a disk on OS X using *hdiutil* (/dev/rdiskX) and then *diskutil* to mount the filesystems on OS X.

```
# fs_univ mount -l 192.168.1.83 -s win10-x64-dev -t DiscoveryShare-C -m . -d
  F-Response Universal Linux Examiner 2.0.1.15
  Copyright F-Response, All Rights Reserved
  Checking appliance '192.168.1.83' connection status ... success
  Locating subject 'win10-x64-dev' on appliance '192.168.1.83' ... success
  Locating target 'DiscoveryShare-C' on subject 'win10-x64-dev' ... success
  Pushing target mount path on '/root/Desktop' ... success
  Connected to appliance 192.168.1.83.
  Connected to target DiscoveryShare-C on subject win10-x64-dev.
  Target DiscoveryShare-C is mounted and process is running in the background.
  Exclude -d,--daemon on command line to run in foreground.
```

umount

The umount command unmounts a target specified by appliance, subject, and target name. This operation is equivalent to running *umount* on the mount path on both Linux and OS X.

```
# fs_univ umount -l 192.168.1.83 -s win10-x64-dev -t DiscoveryShare-C
  F-Response Universal Linux Examiner 2.0.1.15
```

```
  Copyright F-Response, All Rights Reserved
  Successfully unmounted /root/Desktop/win10-x64-dev/DiscoveryShare-C.
```

active

The active command prints a list of mounted targets in either CSV or JSON format.

```
 # fs_univ active
   appliance_name,subject_name,target_name,target_type,target_size,block_size,block_count,mount_path
   192.168.1.83,win10-x64-dev,DiscoveryShare-C,share,119GB,4096,31431167,/root/.../…/DiscoveryShare-C
```

```
# fs_univ –json
   {
       "192.168.1.83": {
           "win10-x64-dev": [
               {
                   "block_count": "31431167",
                   "block_size": "4096",
                   "case_sensitive": "0",
                   "mount_path": "/root/Desktop/win10-x64-dev/DiscoveryShare-C",
                   "name": "DiscoveryShare-C",
                   "pid": "3941",
                   "root_node": "5",
                   "type": "2",
                   "uuid": "1"
               }
           ]
       }
   }
```

The subject should now be visible in the F-Response Universal console on the examiner machine.

Appendix A.

Legal Notices

Trademarks

F-Response, DiscoveryShare, and MemoryShare, are trademarks of Agile Risk Management, LLC. All other product names or logos mentioned herein are used for identification purposes only, and are the trademarks of their respective owners.

Statement of Rights

Agile Risk Management, LLC products incorporate technology that is protected by U.S. patent and other intellectual property (IP) rights owned by Agile Risk Management LLC, and other rights owners. Use of these products constitutes your legal agreement to honor Agile Risk Management, LLC's IP rights as protected by applicable laws. Reverse engineering, de-compiling, or disassembly of Agile Risk Management, LLC products is strictly prohibited.

Disclaimer

While Agile Risk Management LLC has committed its best efforts to providing accurate information in this document, we assume no responsibility for any inaccuracies that may be contained herein, and we reserve the right to make changes to this document without notice.

Patents

F-Response is covered by United States Patent Numbers: 8,171,108; 7,899,882; 9,037,630; and other Patents Pending.

Appendix B.

Release History

8.7.1.27 -> Corrected issue with Dropbox for Business Team Folder collection.

8.7.1.19 -> Change Product Summary Information during MSI export to match product and manufacturer as provided.

8.7.1.17 -> Minor corrections to Cloud Files collections to confirm they match existing mission guide documentation.

8.7.1.9/8.7.1.10/8.7.1.11 -> Added support for Google Compute under Cloud Servers. Changed interface to reflect Google Workspace as opposed to GSuite. Added an option to export CSV of Subject and Examiner history to the F-Response Configuration Console.

8.6.1.4 -> Corrected F-Response Box.com collection to use localhost instead of 127.0.0.1 as per recent change at Box. Updated EC2 Cloud Server collection to prompt for one or more regions prior to collection.

8.5.1.14 -> Corrected issue with running Agentless, Cloud Servers, and Cloud Files collection. Added capability to locate and properly handle Dropbox for Business Teams Folders. Disabled web configuration pages by default. To re-enable web pages for configuration until they are removed at a later date, add “webremove”:false, to your fresuniv.cfg and restart.

8.5.1.10/8.5.1.11/8.5.1.12 -> Removed the VHD subsystem for Agentless, Cloud Servers, and Cloud Files collection. Corrected an issue with Dropbox refresh token acquisition. Corrected alternate hostname assignment in MSI export. Added subjectthreshold option for certain support situations.

8.4.1.3 -> Added new F-Response Cloud Servers data source. F-Response can now collect cloud server volume snapshots from Amazon and Azure. For more details, see the mission guides on our website. Adjusted F-Response Cloud File collections to use explicit volume mount point (UUID) to reduce potential for pathing errors for certain collections.

8.3.1.19 -> Altered IP restrictions to allow ranges as well as individual addresses. Corrected mission system token authentication when user accounts or passwords contained non-printable characters. Addressed 3rd party library issue with https requests for cloud collection.

8.3.1.14/8.3.1.15 -> Corrected issue with universal subject attempting to connect when no devices were detected. Corrected directory traversal issue with Discoveryshares and a specific character combination. Corrected UI misspelling in the server configuration tool. Corrected issue with SSH key authentication and Agentless collections.

8.3.1.12 -> Added new F-Response Universal Server configuration tool and option to remove web administration interface. Web interface will be deprecated and removed in a future release. Added new iprestrictions options for optionally reducing examiner connections to a specific list of IP addresses.

8.3.1.8 -> Revised internal RPC model for ease of troubleshooting, added additional cloud collection checks to prohibit running two collections at the same time for a single credential, added token refresh checks based on published cloud provider status codes (400, 401, etc), added fallback option for deployment in the event newly added security descriptors fail, added quotes around service install exe paths.

8.3.1.6 -> Added restart options for failed physical device image (after device has been reattached). Added new security controls around deployment share creation.

8.2.1.14 ->Corrected issue with Universal Server including non-functional crypto suites for TLS that could result in failed TLS sessions. Improved error handling for failed windows deployment operations.

8.2.1.5 -> Corrected issue with Universal Server installer not overwriting past installs correctly.

8.2.1.4 -> Added browse options for configuring cloud collections, added GSuite log collection, and addressed issue with OneDrive alternate root selection.

8.1.1.4 -> Added new Agentless Connection Collection features and correct csv file destination for cloud collections not saved to a VHD.

8.0.1.77 -> Added re-run options for collecting certain cloud providers, documented log entries, and added error codes for licensing operation failures.

8.0.1.69 -> Corrected token refresh for JWT Tokens in GSuite.

8.0.1.68 -> Added new cloud collection options including alternate root selection, file name filtering, and optional recursion. Fixed Dropbox for Business and Box.com for Business to display the custodian email and not the provider specific id.

8.0.1.62 -> Corrected an issue with the Universal examiner UI that created instability during universal server add and remove operations.

8.0.1.58 -> Corrected an issue in the Universal Server that resulted in duplicate subjects appearing when passive TCP disconnects were not detected. Updated the Windows Universal Examiner tools to detect a loss of connectivity to the Universal server and adjust the interface accordingly. Enforced TLSv1.2 in all HTTPS connections to the Universal server. Corrected a UI issue when deleting cloud storage accounts and for handling menus in multiple monitor configurations.

8.0.1.55 -> Corrected an issue with the newly added deployment option.

8.0.1.54 -> Brought back the Mission System as well as deploy as current user. Corrected issue with stale cache details that would often present an inaccurate view of the subjects currently communicating with the Universal Server.

8.0.1.46 -> Corrected issue with GSuite custodian enumeration. Changed Amazon S3 bucket collection to use v4 signatures. Fixed issue with non-windows subject deployment.

8.0.1.44 -> Added display filtering to the Windows F-Response Universal Management Console. Improved cloud collection performance for large custodian organizations and added custodian selection by email address for Office 365.

8.0.1.42 -> Initial release for the 8.x series. This version brings Universal in line with other F-Response products in terms of display and interfaces.

2.0.1.17 -> Improved handling for > 2TB subject devices. Improved the command line tool for managing users (fswitchadm).

2.0.1.16 -> Corrected fragmented read issue when making unusually large read requests. Updated the Universal appliance to handle Amazon Ec2 licensing. Completely redesigned Linux and OSX examiner software.

2.0.1.12 -> Corrected user interface issue when opening multiple devices simultaneously. Updated the Linux subject executable to handle more diverse device targets. Improvements to the Linux and Apple OSX examiner to correct authentication issue. Improvements to the Active Directory/LDAP authentication process allowing for success in more complex environments.

2.0.1.11 -> Updated F-Response Universal deployment processes to handle the recent changes in Apple OSX El Capitan. Additional minor user interface corrections.

2.0.1.6 -> Updated F-Response Universal User Interfaces (Now and Universal) for more efficient usage. Additional icons, grids, and layout to provide for an easier user experience. Modifications to the LDAP authentication system allowing for more diverse Domain authentication scenarios. Additional Examiner software packages for Apple OSX and Linux. Minor adjustments to the Mission System to address ipv6 address differences. Modifications to the F-Response Universal Subject software for Windows to reduce potential for hibernation and sleep while actively mounted.

1.0.75.7 -> Corrected issues with remote DiscoveryShare name content filtering. Upgraded the F-Response F-Switch SCSI Adapter to address a timing issue during drive attach/detach operations. Added a complete LDAP configuration testing tool to address issues with properly configuring LDAP authentication. Added additional options in configuration to handle IPv4/IPv6 socket binding.

1.0.75.6 -> Addressed issues with remote DiscoveryShare content that violates Windows naming conventions. Modified the physical drive numbering detection model. Improved LDAP authentication model to better handle complex LDAP configurations.

1.0.75.5 -> Updated F-Response Universal and Now clients to better detect spurious memory reservations, address internal drive and volume access authentication inconsistencies. Updated F-Response Universal and Now appliance software to improve LDAP/Active Directory integration, better handle systems with modified tcp ports. Updated F-Response Univ/Now Linux examiner to reduce 3rd party dependencies and streamline configuration. Libconfig dropped in favor of Lua style configuration and additional build platform included, Centos 7. Updated Android apk build to improve performance based on internal testing and user feedback. Windows F-Response Univ/Now console improvements for stability.

1.0.75.4 -> Updated F-Response F-Switch SCSI driver to revision 4. Improved stability and performance in high speed IO operations. Modified worker process to improve stability and memory consumption in high speed IO operations.

1.0.75.3 -> Modifications to the internal F-Response Univ/Now architecture to improve data transmission speed and performance.

1.0.75.2 -> Modifications to the examiner driver stack to improve performance, stability, and reduce potential for device timeout.

1.0.75.1 -> Modifications to subject executables to include dynamic reconnection to Univ/Now, additional keep-alive improvements to long haul network links, read timeouts and stability updates.

1.0.74.8 -> Modifications to address worker process loading in non-standard operating environments.

Initial Release -> 1.0.74.7

Appendix C.

Master Software License Agreement

AGILE RISK MANAGEMENT LLC MASTER SOFTWARE LICENSE AGREEMENT

TERMS AND CONDITIONS

1. Scope of Agreement; Definitions. This Agreement covers the license and permitted use of the Agile Risk Management LLC ("Agile") F-Response Software. Unless otherwise defined in this section, the capitalized terms used in this Agreement shall be defined in the context in which they are used. The following terms shall have the following meanings:

1.1. "Agile Software" or "Software" means any and all versions of Agile's F-Response software and the related "Documentation" as defined below.

1.2. "Customer" or "Licensee" means the person or entity identified on the invoice and only such person or entity, Customer shall not mean any assigns, heirs, or related persons or entities or claimed third-party beneficiaries of the Customer.

1.3. "Documentation" means Agile release notes or other similar instructions in hard copy or machine readable form supplied by Agile to Customer that describes the functionality of the Agile Software.

1.4. "License Term" means the term of the applicable license as specified on an invoice or as set forth in this Agreement.

2. Grant of Software License.

2.1. Enterprise License. Subject to the terms and conditions of this Agreement only, Agile grants Customer a non-exclusive, non-transferable license to install the Agile Software and to use the Agile Software during the License Term, in object code form only.

2.2. Third Party Software. Customer acknowledges that the Agile Software may include or require the use of software programs created by third parties, and the Customer acknowledges that its use of such third party software programs shall be governed exclusively by the third party's applicable license agreement.

3. Software License Restrictions.

3.1. No Reverse Engineering; Other Restrictions. Customer shall not, directly or indirectly: (i) sell, license, sublicense, lease, redistribute or transfer any Agile Software; (ii) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, or distribute any Agile Software; (iii) rent or lease any rights in any Agile Software in any form to any entity; (iv) remove, alter or obscure any proprietary notice, labels or marks on any Agile Software. Customer is responsible for all use of the Software and for compliance with this Agreement and any applicable third party software license agreement.

3.2. Intellectual Property. Agile retains all title, patent, copyright and other intellectual proprietary rights in, and ownership of, the Agile Software regardless of the type of access or media upon which the original or any copy may be recorded or fixed. Unless otherwise expressly stated herein, this Agreement does not transfer to Customer any title, or other ownership right or interest in any Agile Software. Customer does not acquire any rights, express or implied, other than those expressly granted in this Agreement.

4. Ordering & Fulfillment. Unless otherwise set forth in an Agile-generated Estimate pricing is set forth on the F-Response website and is subject to change at any time. Each order shall be subject to Agile's reasonable acceptance. Unless otherwise set forth in an Agile generated Estimate. Delivery terms are FOB Agile's shipping point.

5. Payments. Customer agrees to pay amounts invoiced by Agile for the license granted under this Agreement. If any authority imposes a duty, tax or similar levy (other than taxes based on Agile's income), Customer agrees to pay, or to promptly reimburse Agile for, all such amounts. Unless otherwise indicated in an invoice, all Agile invoices are payable thirty (30) days from the date of the invoice. Agile reserves the right to charge and Customer agrees to pay Agile for every unauthorized copy or unauthorized year an amount equal to the cost per copy, per year, per computer, or per user, whichever is greater, as a late payment fee in the event Customer fails to remit payments when due or Customer otherwise violates the payment provisions of this Agreement. In addition to any other rights set forth in this Agreement, Agile may suspend performance or withhold fulfilling new Customer orders in the event Customer has failed to timely remit payment for outstanding and past due invoices.

6. Confidentiality.

6.1. Definition. "Confidential Information" means: (a) any non-public technical or business information of a party, including without limitation any information relating to a party's techniques, algorithms, software, know-how, current and future products and services, research, engineering, vulnerabilities, designs, financial information, procurement requirements, manufacturing, customer lists, business forecasts, marketing plans and information; (b) any other information of a party that is disclosed in writing and is conspicuously designated as "Confidential" at the time of disclosure or that is disclosed orally and is identified as "Confidential" at the time of disclosure; or (c) the specific terms and conditions of this Agreement.

6.2. Exclusions. Confidential Information shall not include information which: (i) is or becomes generally known to the public through no fault or breach of this Agreement by the receiving Party; (ii) the receiving Party can demonstrate by written evidence was rightfully in the receiving Party's possession at the time of disclosure, without an obligation of confidentiality; (iii) is independently developed by the receiving Party without use of or access to the disclosing Party's Confidential Information or otherwise in breach of this Agreement; (iv) the receiving Party rightfully obtains from a third party not under a duty of confidentiality and without restriction on use or disclosure, or (v) is required to be disclosed pursuant to, or by, any applicable laws, rules, regulatory authority, court order or other legal process to do so, provided that the Receiving Party shall, promptly upon learning that such disclosure is required, give written notice of such disclosure to the Disclosing Party.

6.3. Obligations. Each Party shall maintain in confidence all Confidential Information of the disclosing Party that is delivered to the receiving Party and will not use such Confidential Information except as expressly permitted herein. Each Party will take all reasonable measures to maintain the confidentiality of such Confidential Information, but in no event less than the measures it uses to protect its own Confidential Information. Each Party will limit the disclosure of such Confidential Information to those of its employees with a bona fide need to access such Confidential Information in order to exercise its rights and obligations under this Agreement provided that all such employees are bound by a written non-disclosure agreement that contains restrictions at least as protective as those set forth herein.

6.4. Injunctive Relief. Each Party understands and agrees that the other Party will suffer irreparable harm in the event that the receiving Party of Confidential Information breaches any of its obligations under this section and that monetary damages will be inadequate to compensate the non-breaching Party. In the event of a breach or threatened breach of any of the provisions of this section, the non-breaching Party, in addition to and not in limitation of any other rights, remedies or damages available to it at law or in equity, shall be entitled to a temporary restraining order, preliminary

injunction and/or permanent injunction in order to prevent or to restrain any such breach by the other Party.

7. DISCLAIMER OF WARRANTIES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AGILE AND ITS SUPPLIERS PROVIDE THE SOFTWARE AND SUPPORT SERVICES (IF ANY) AS IS AND WITH ALL FAULTS, AND HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY (IF ANY) IMPLIED WARRANTIES, DUTIES OR CONDITIONS OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF RELIABILITY OR AVAILABILITY, OF ACCURACY OR COMPLETENESS OF RESPONSES, OF RESULTS, OF WORKMANLIKE EFFORT, OF LACK OF VIRUSES, AND OF LACK OF NEGLIGENCE, ALL WITH REGARD TO THE SOFTWARE, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE SOFTWARE.

8. Limitations and Exclusions.

8.1. Limitation of Liability and Remedies. NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED ABOVE AND ALL DIRECT OR GENERAL DAMAGES IN CONTRACT OR ANY OTHER THEORY IN LAW OR IN EQUITY), THE ENTIRE LIABILITY OF EITHER PARTY AND WITH RESPECT TO AGILE, ANY OF ITS SUPPLIERS, UNDER ANY PROVISION OF THIS AGREEMENT AND THE EXCLUSIVE REMEDY HEREUNDER SHALL BE LIMITED TO THREE TIMES THE TOTAL AMOUNT PAID BY CUSTOMER FOR THE LICENSE; PROVIDED, HOWEVER THAT THIS LIMITATION DOES NOT APPLY TO ANY OF THE FOLLOWING: (A) A PARTY'S BREACH OF ITS CONFIDENTIALITY OBLIGATIONS UNDER THIS AGREEMENT; OR (B) ANY GROSS NEGLIGENCE OR WILLFUL MISCONDUCT BY A PARTY. THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS ITS ESSENTIAL PURPOSE.

8.2. Exclusion of Incidental, Consequential and Certain Other Damages. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY, AND WITH RESPECT TO AGILE, ITS SUPPLIERS, BE LIABLE TO THE OTHER FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF AGILE OR ANY SUPPLIER, AND EVEN IF AGILE OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR TO ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL, DAMAGES (INCLUDING WITHOUT LIMITATION, LIABILITIES RELATED TO A LOSS OF USE, PROFITS, GOODWILL OR SAVINGS OR A LOSS OR DAMAGE TO ANY SYSTEMS, RECORDS OR DATA), WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED IN ADVANCE OR AWARE OF THE POSSIBILITY OF ANY SUCH LOSS OR DAMAGE. THE FOREGOING LIMITATIONS OF LIABILITY WILL NOT APPLY TO ANY OF THE FOLLOWING: (A) A PARTY'S BREACH OF ITS CONFIDENTIALITY OBLIGATIONS UNDER THIS AGREEMENT; OR (B) ANY GROSS NEGLIGENCE OR WILLFUL MISCONDUCT BY A PARTY.

8.3. Indemnification. Licensor hereby agrees to indemnify, hold harmless and defend Licensee and any partner, principal, employee or agent thereof against all claims, liabilities, losses, expenses (including attorney's fees and legal expenses related to such defense), fines, penalties, taxes or damages (collectively "Liabilities") asserted by any third party where such Liabilities arise out of or result from: (1) any claim that the Software or Customer's use thereof violates any copyright, trademark, patent and/or any other intellectual property rights; (2) the negligence of Licensor in the course of providing any Services hereunder; or (3) the representations or warranties made by Licensor hereunder, or their breach. Licensee shall promptly notify Licensor of any third party claim and Licensor shall, at Licensee's option, conduct the defense in any such third party action arising as described herein at Licensor's sole expense and Licensee shall cooperate with such defense.

9. Verification.

9.1. Agile has the right to request Customer complete a self-audit questionnaire in a form provided by Agile. If an audit reveals unlicensed use of the Agile Software, Customer agrees to promptly order and pay for licenses to permit all past and ongoing usage.

10. Support Services

10.1. Rights and Obligations. This Agreement does not obligate Agile to provide any support services or to support any software provided as part of those services. If Agile does provide support services to you, use of any such support services is governed by the Agile policies and programs described in the user manual, in online documentation, on Agile's support webpage, or in other Agile-provided materials. Any software Agile may provide you as part of support services are governed by this Agreement, unless separate terms are provided.

10.2. Consent to Use of Data. You agree that Agile and its affiliates may collect and use technical information gathered as part of the support services provided to you, if any, related to the Software. Agile may use this information solely to improve our products or to provide customized services or technologies to you and will not disclose this information in a form that personally identifies you.

11. Miscellaneous.

11.1. Legal Compliance; Restricted Rights. Each Party agrees to comply with all applicable Laws. Without limiting the foregoing, Customer agrees to comply with all U.S. export Laws and applicable export Laws of its locality (if Customer is not located in the United States), and Customer agrees not to export any Software or other materials provided by Agile without first obtaining all required authorizations or licenses. In the event the Software is provided to the United States government it is provided with only "LIMITED RIGHTS" and "RESTRICTED RIGHTS" as defined in FAR 52.227-14 if the commercial terms are deemed not to apply.

11.2. Governing Law; Severability. This Agreement (including any addendum or amendment to this Agreement which is included with the Software) are the entire agreement between you and Agile relating to the Software and the support services (if any) and they supersede all prior or contemporaneous oral or written communications, proposals and representations with respect to the Software or any other subject matter covered by this Agreement. To the extent the terms of any Agile policies or programs for support services conflict with the terms of this Agreement, the terms of this Agreement shall control. This Agreement shall be governed by the laws of the State of Florida, USA, without regard to choice-of-law provisions. You and Agile agree to submit to the personal and exclusive jurisdiction of the Florida state court located in Tampa, Florida, and the United States District Court for the Middle District of Florida. If any provision of this Agreement is held to be illegal or unenforceable for any reason, then such provision shall be deemed to be restated so as to be enforceable to the maximum extent permissible under law, and the remainder of this Agreement shall remain in full force and effect. Customer and Agile agree that this Agreement shall not be governed by the U.N. Convention on Contracts for the International Sale of Goods.

11.3. Notices. Any notices under this Agreement will be personally delivered or sent by certified or registered mail, return receipt requested, or by nationally recognized overnight express courier, to the address specified herein or such other address as a Party may specify in writing. Such notices will be effective upon receipt, which may be shown by confirmation of delivery.

11.4. Assignment. Customer may not assign or otherwise transfer this Agreement without the Agile's prior written consent, which consent shall not be unreasonably withheld, conditioned or delayed. This Agreement shall be binding upon and inure to the benefit of the Parties' successors and permitted assigns, if any.

11.5. Force Majeure. Neither Party shall be liable for any delay or failure due to a force majeure event and other causes beyond its reasonable control. This provision shall not apply to any of Customer's payment obligations.

11.6. Redistribution Compliance.

(a) F-Response distributes software libraries developed by The Sleuth Kit ("TSK"). The license information and source code for TSK can be found at http://www.sleuthkit.org/. If any changes have been made by Agile to the TSK libraries distributed with the F-Response software, those changes can be found online at http://www.f-response.com/TSKinfo.

(b) A portion of the F-Response Software was derived using source code provided by multiple 3rd parties which requires the following notices be posted herein, and which applies only to the source code. F-Response code is distributed only in binary or object code form. F-Response source

code, and any revised 3rd party code contained within the F-Response source code, is not available for distribution. The name of 3rd parties included below are not being used to endorse or promote this product, nor is the name of the author being used to endorse or promote this product. This information is presented solely to comply with the required license agreements which require reproduction of the following copyright notice, list of conditions and disclaimer:

Copyright (c) 2009-2014 Petri Lehtinen <petri@digip.org>

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER

LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young
eay@cryptsoft.com). This product includes software written by Tim
Hudson (tjh@cryptsoft.com).

Intel License Agreement

Copyright (c) 2000, Intel Corporation

All rights reserved.

- Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- The name of Intel Corporation may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright © 2006 Alistair Crooks. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2011-2014, Loïc Hoguin <essen@ninenines.eu>

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright 2009-2011 Andrew Thompson <andrew@hijacked.us>. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE PROJECT ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2000-2010 Marc Alexander Lehmann <schmorp@schmorp.de>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

11.7. General. This Agreement, including its exhibits (all of which are incorporated herein), are collectively the Parties' complete agreement regarding its subject matter, superseding any prior oral or written communications. Amendments or changes to this Agreement must be in mutually executed writings to be effective. The Parties agree that, to the extent any Customer purchase or sales order contains terms or conditions that conflict with, or supplement, this Agreement, such terms and conditions shall be void and have no effect, and the provisions of this Agreement shall control. Unless otherwise expressly set forth in an exhibit that is executed by the Parties, this Agreement shall control in the event of any conflict with an exhibit. Sections 2, 3, 5, 7, 8, and 9, and all warranty disclaimers, use restrictions and provisions relating to Agile's intellectual property ownership, shall survive the termination or expiration of this Agreement. The Parties are independent contractors for all purposes under this Agreement.

11.8. Changes to this agreement. Agile will entertain changes to this agreement on a case by case basis. Changes to this Agreement may require that the Customer pay an additional administrative fee depending on the scope and complexity of the changes required by the Customer. The additional administrative fee, if any, must be paid before the license will be activated.

Appendix D

Alternate SSL Certification Configuration

F-Response Universal provides a generic SSL certificate and private key for securing Admin/Web access to the server, however, you may replace these values with your own certificate and key. Generating a certificate and private key is outside the scope of this document. For the purposes of this appendix we will assume you have a certificate file and corresponding private key.

You will need to place both files in an accessible directory. We recommend placing them outside the program files folder as the contents of this directory may change with new installations of F-Response Universal. Once you have selected or created the directory you will need to place the certificate and private key file in the directory, and then locate the fresuniv.cfg file. This file should be located in the original F-Response Universal installation directory.

This file is in JSON format.

You will need to add the following entries to the file and restart the F-Response Universal Service to change the SSL certificate used.

"sslcert":"C:\\path\\to\\cert.crt","sslkey":"C:\\path\\to\\private.key"

Appendix E

Log Formats

The following log formats are available:

- Standard (CSV)
  - function, username, datetime, type, message
- QRadar
  - datetime, Hostname LEEF:1.0|F-Response|F-Response Universal|8.0|INFO|function=,username=,type=,message=
- Splunk
  - datetime, hostname=,function=,username=,type=,message=

Function	**removedomain**
Content	Removed Active Directory Domain <DOMAIN>.
Reason	Indicates when an Active Directory login Domain has been removed.

Function	**adddomain**
Content	Added Active Directory Domain <DOMAIN>.
Reason	Indicates when an Active Directory login Domain has been added.

Function	**testdomain**
Content	Testing <DOMAIN\USERNAME>'s AD Domain.
Reason	Indicates when the Universal is testing whether the user resides in that domain and the configured groups.

Function	**validateaduser**
Content	Validated Active Directory user <USERNAME>. Unable to validate <USERNAME>, error <ERROR>.
Reason	Indicates success or failure in validating a user against the configured Active Directory.

Function	**getusertoken**
Content	Login user <USERNAME> successful.
Reason	Indicates successful login.

Function	**verifytoken**
Content	Unable to verify token, error <ERROR>. Verified token from local system for user <USERNAME>.
Reason	Indicates successful verification of a token.

Function	**setauthtype**
Content	Successfully set auth type to <AUTHTYPE>. Failed to set authtype <AUTHTYPE>, error <ERROR>. Failed to set authtype <AUTHTYPE>, not a valid authtype.
Reason	Indicates success or failure in setting authorization type.

Function	**adduser**
Content	Added user <USERNAME>, role <ROLE>.
Reason	Indicates success in adding a user.

Function	**removeuser**
Content	Removed user <USERNAME>.
Reason	Indicates success in removing a user.

Function	**listusers**
Content	Listed users.
Reason	Lists users (only valid with local users).

Function	**changeuserrole**
Content	Changed user <USERNAME> role to <ROLE>.
Reason	Indicates changed user role (only valid with local users).

Function	**changeuserpassword**
Content	Changed user <USERNAME> password.
Reason	Indicates changed user password (only valid with local users).

Function	**changeownpassword**
Content	Changed user <USERNAME> password.
Reason	Indicates changed own password (only valid with local users).

Function	**load_der**
Content	Unable to load <DERFILE>, error <ERROR>. Unable to read registry value <REGISTRY> der, error <ERROR>. Unable to open registry <REGISTRY>, error <ERROR>. Unable to open DER file <DERFILE>, error <ERROR>.
Reason	These messages indicate errors with loading the cryptography parameters.

Function	**validate_license**
Content	License validation error <ERROR> with reason <REASON>.
Reason	Indicates an error during license validation with license.f-response.com.

Function	**configureproxy**
Content	Set proxy host to <PROXYHOST> and port to <PROXYPORT>.
Reason	Indicates setting the proxy host and port.

Function	**setlogtype**
Content	Changed logtype to <LOGTYPE> and loglocation to <LOGLOCATION>.
Reason	Indicates setting the log type.

Function	**setoperatingmode**
Content	Set to standard. Set to filtered.
Reason	Indicates setting the operating mode to standard or filtered.

Function	**enablefilter**
Content	Set filter <FILTER>.
Reason	Indicates setting the filter to a new value.

Function	**disablefilter**
Content	Disabled filter.
Reason	Indicates clearing the filter and removing all connected machines.

Function	**listcurrentsubjects**
Content	Listed current subjects.
Reason	Indicates listing the currently connected subjects.

Function	**listcurrentexaminers**
Content	Listed current examiners.
Reason	Indicates listing the currently connected examiners.

Function	**purgesubjects**
Content	Remove subject history.
Reason	Indicates removing the subject history.

Function	**purgeexaminers**
Content	Remove examiner history.
Reason	Indicates removing the examiner history.

Function	**listsubjects**
Content	Listed subjects.
Reason	Indicates listing historical subjects.

Function	**listexaminers**
Content	Listed examiners.
Reason	Indicates listing historical examiners.

Function	**match**
Content	Subject <SUBJECT> matched <FILTER>.
Reason	Indicates a subject has connected and matched the filter.

Function	**register_exa**
Content	Examiner <USERNAME> has connected from <IP>. License file error <ERROR>.

Reason	Indicates success or failure for connecting an examiner management console.

Function	**safe_sub_targ_login_resp_info_message_send**
Content	Disconnected session due to an inability to locate <SUBJECTADDRESS>
Reason	Indicates an inability for Universal to locate the missing subject.

Function	**websocket_info**
Content	Operation timed out before response was received.
Reason	Indicates a timeout in waiting for a subject response.

Function	**subject_exit**
Content	Subject <HOSTNAME> from <IP> has disconnected.
Reason	Indicates the subjects has disconnected from the universal server.

Function	**getmissions**
Content	Examiner retrieved list of missions.
Reason	Indicates an examiner has retrieved the list of missions.

Function	**newmission**
Content	Examiner created new mission <MISSION>.
Reason	Indicates an examiner has created a new mission.

Function	**deletemission**
Content	Examiner successfully deleted mission <MISSION>.
Reason	Indicates an examiner has successfully deleted a mission.

Function	**verifysubjectmission**
Content	Subject <SUBJECT> is a match for a mission.
Reason	Indicates a subject is a match for a mission.

Function	**clearfilter**
Content	Cleared filter.
Reason	Indicates the filter has been cleared.

Function	**listfiltered**
Content	Testing subjects against existing filter.
Reason	Indicates testing the subjects against an existing filter.